Order ID: **4QBA57113850** Mod: 011, Ver:03 Date: September 6, 2016	Servicing Agency: General Services Administration FAS/AASD/Branch B, Suite 2700 401 West Peachtree Street Atlanta, GA 30308 Customer Account Manager: Kevin G. Metcalf Phone: (b) (6) Email: kevin.metcalf@gsa.gov ~~Patrick Scanlon~~ ~~Phone:~~ (b) (6) ~~Fax: (912) 634 2200 (fax)~~ ~~E-Mail: patrick.scanlon@gsa.gov~~ Senior Contracting Officer: Keith C. Echols Phone: (b) (6) Email: keith.echols@gsa.gov ~~Garett Nelson~~ ~~Phone:~~ (b) (6) ~~E-mail: garett.nelson@gsa.gov~~
Client Org: AFRC (Air Force Reserve Command) 155 Richard Ray Blvd, Bldg 210 Robins AFB, GA 31098 -1655	Client Rep/COR: Teresa A Bryant Phone: (b) (6) Email: teresa.bryant@us.af.mil ~~CMSgt Thomas Henry~~ ~~Phone:~~ (b) (6) ~~Fax: (478) 327 0448~~ ~~Email: thomas.henry@us.af.mil~~
Project Name: **Global Command and Control and IT Support HQ AFRC** ~~**AFRC Headquarters (HQ) and Communications Support**~~	Period of Performance: 09/29/2011 – 03/28/2017 Base Year: 09/29/2011 – 09/28/2012 OY 1: 09/29/2012 -09/28/2013 OY 2: 09/29/2013 – 09/28/2014 OY 3: 09/29/2014 – 09/29/2015 OY 4: 09/29/2015 – 09/28/2016 Extension: 09/29/2016 – 03/28/2017
Contract Type: ALLIANT GWAC Task Order Performance Based Firm Fixed Price / Time and Materials Severable Incrementally Funded	Vendor: General Dynamics One Source LLC Business Address: 3211 JERMANTOWN ROAD, FAIRFAX, VA 22030-2844 Contractor Rep: Leslie A Miles Phone: (b) (6) E-Mail: leslie.miles@gdit.com Contract #: GS00Q09BGD0030

Modifications and Change LOG: (All changes are noted in Bold Red Text)

Mod #	Date	Description
011	**TBD**	**The purpose of this modification is to realign $25K from excess T&M labor and increase OY4 Travel Budget, Extend support services for 6 months, remove support services for Pope AFB effective 09/29/2016, remove excess requirements and funding from the completed period of performance, make Admin Mod changes change COR, SCO and CAM, and make those changes as noted in PWS sections: Summary Header, Mod Change Log, 2.4, 5.3, 5.4, 5.19.5, 5.21.6, Appendix: Tables 3, 4, 5, 6, 7, and 8 Request for CAC.**
010	**12/16/2015**	Modification 010 is issued to add Contractor Manpower Reporting (via eCMRA) requirements to the task order in accordance with PWS paragraph(s) 5.11.14 – 5.11.14.3. Modification 010 will also clarify PWS paragraph 5.5.1 to include and address contractor use of government leased vehicles. All changes are highlighted in RED font in their corresponding paragraphs below
009	**09/11/2015**	Modification 009 is issued to execute Option Year four (4) of the task order; Period of Performance (POP) dates 09/29/2015 – 09/28/2016.
008	**02/26/2015**	Modification 008 will incorporate the following changes into the task order, highlighted in RED font throughout the PWS:

1. Formally names and provides contact information for the GSA Senior Contracting Officer.
2. Scope verbiage changes, PWS paragraph 1.1, “This contract…changed to This Task Order…”
3. The term “Vendor Program Manager” is hereby changed to “On-Site Project Manager” in PWS paragraphs 1.3 and 5.22. The requirements of PWS pp 1.3.2 are clarified and highlighted in red FONT below in the applicable paragraph.
4. Clarifies requirements for Privileged Access Agreements (PAA) in accordance with PWS pp 1.3.2.
5. Requires additional detailed information to be delivered with Monthly Financial Summary (MFS) Report, PWS pp 1.4.5.
6. Changes to PWS pp 2.3 clarify enhanced requirements and removes requirement for vendor to maintain an “offsite facility”.
7. Removes requirement for Legacy SCCM, PWS pp 2.3.2.1.
8. Adds requirement for Vulnerability Management Server/Workstation Support PWS pp 2.3.2.10.
9. Increases level of support required in PWS pp 2.3.3.

10. De-scopes requirements of PWS pp 2.3.3.1.
11. Clarifies services required in PWS pp 2.4.2 and 2.5.
12. Updates tracking status requirements PWS pp (2.5.2.8.);
13. Updates numbers and clarifies duties of the VTC; changes name of VTC to reflect VTC Operations Center (2.5.3. thru 2.5.3.3.).
14. Changes name from SharePoint to SharePoint Administrator (2.5.5.).
15. Changes all references from SOA to reflect Service Oriented Cloud Environment (SOCE)
16. Clarifies description, current state, and requirement (2.5.6.3.1. thru 2.5.6.3.1.5.2.).
17. Updates project background verbiage on GCCS responsibilities (3.).
18. Updates buildings supported on Robins AFB, GA (3.1.3.).
19. Changes name of IT Consultant to reflect IT Requirements Support; aligns duties to actual requirements (4.2.).
20. Adds VOIP requirements and updates skill-sets and deliverables (4.3.).
21. Changes name of Dashboard to reflect Internal Control Measures (ICM); updates deliverables (4.5. and 4.6.).
22. Revises PWS pp 4.7 – 4.7.9.9 and increases the level of support required for Enterprise Architecture (EA) Program Analysts.
23. De-scopes PWS pp 4.10, 4.10.1, Cyber PIO Action Officer Requirements.
24. New Support Requirement PWS pp 4.22, Cyber Force Readiness.
25. New Support Requirement PWS pp 4.23, Master Calendar Functional Administrator.
26. De-scopes the Chief Technology Officer (CTO) Support Analyst requirements.
27. Updates duties of Cyber Force Readiness PWS pp 4.22.
28. Updates the requirements of Master Calendar Functional Administrator duties to this task order PWS pp (4.23.).
29. Adds additional FAR/AFFAR directives PWS pp 5.1.
30. Clarifies that the contractor is permitted to ride as a passenger in GSA leased vehicles at any time (5.5.1.).
31. Clarifies hours of work; telecommuting; and requirement for task order support on UTA weekends (5.6.1.).
32. Clarifies guidance on overtime/extended hours, PWS pp (5.6.3.).
33. Clarifies contractor recall; authorized creation of "on-call" rosters PWS pp (5.7.).
34. Clarifies telecommuting; specifies that the COR and GSA Contracting Officer are the approving officials for all telecommuting and work agreements PWS pp 5.8.1 - 5.8.2.
35. Removes requirement to issue Government purchased/support cell phone to contractors PWS pp 5.10.2.
36. Clarifies verbiage; includes some annual training requirements of contractors PWS pp 5.11.1.
37. Clarifies that all data created, regardless of media, is the property of the Government PWS pp 5.11.2.
38. Clarifies requirements and adds additional verbiage for physical and information security PWS pp 5.11.9.1. thru 5.11.9.3.2.
39. Clarifies additional clarification on Privacy Act information PWS pp 5.11.10.
40. Clarifies CAC processing procedures for all contractors on this task order PWS pp 5.11.12.
41. Clarifies Performance/Deliverable metrics PWS pp 5.16; updates compliance documents (5.18., Table 2).
42. Updates GSA website PWS pp 5.19.4.

43. Adds additional FAR references PWS pp 5.21.6.
44. Updates terminology; changes all references from “Client Representative” to reflect “COR” (5.22.).
45. Adds inclement weather verbiage PWS pp 5.23.
46. Adds Federal Holiday verbiage PWS pp 5.24.
47. Adds Family, Energy Conservation, and Early Release Days verbiage PWS pp 5.25.
48. Adds Safety verbiage PWS pp 5.26. thru 5.26.6.
49. Updates acronyms, publications, numbers and locations, and population (Tables 1-7).
50. Updates Request for CAC paperwork (Table 8).
51. Clarifies identified, requires knowledge of PowerShell, VMWare, Hyper-V, TACLANE, Cisco, Remedy, scripting, VOIP, and VOSIP.
52. Makes administrative corrections throughout this entire document.
53. Updates terminology and acronyms.
54. Updates the specific types of operating systems, software, etc…to reflect or generic references.
55. Removes software no longer being used.
56. Identifies cores services to be performed on both NIPRNET and SIPRNET.
57. Removes all references to legacy throughout the PWS.
58. Renumbers the paragraphs, where applicable.
59. Denotes 0 sum FTE swap.

007	**09/18/2014**	Modification 007 exercises Option Year Three (3) of the task order, period of performance dates 09/29/2014 – 09/28/2015.
006	**12/19/2013**	Modification 005 administratively corrects awarded amounts from the basic award, corrected incorrectly in modification 01 and the amounts were incorrectly carried over through modification 02, 03 and 04. The dollar values of funded amounts are unchanged. The lifetime ceiling value and the option year values are corrected by this modification.
005	**09/25/2013**	Incremental funding
004	**09/23/2013**	Modification 004 exercises Option Year Two (2) of the task order, Period of Performance dates 09/29/2013 – 09/28/2014. Modification 004 names a new Contracting Officer for the administration of this task order.
003	09/25/2012	Modification 003 will administratively correct the amounts assigned to task items 003 and 004 during the exercise of Option Year One and also add incremental funding to the task order.
002	**09/20/2012**	Modification 002 exercises Option Year One of the task order, Period of Performance dates 09/29/2012 – 09/28/2013.
001	**08/21/2012**	Modification 001 changes the name of the Customer Account Manager, add the email address of the COR and delete the alternate COR. Mod 001 will also change PWS paragraph 2.4.2 to remove the reference to “Client Onsite Lead” and will increase the requirement for Communication Focal Point (CFP) on-site support at ARPC – Buckley AFB, CO in

		accordance with table 4 below. Modification 001 also adds DFARS Clause 252.209-7999 to PWS paragraph 5.21.5.
000	**09/29/2011**	**Base Award**

PERFORMANCE WORK STATEMENT (PWS)
FOR
GLOBAL COMMAND AND CONTROL AND IT SUPPORT HQ AFRC

1. ORGANIZATION:

DEPARTMENT OF THE AIR FORCE
HQ AIR FORCE RESERVE COMMAND (HQ AFRC)
155 Richard Ray Blvd
ROBINS AFB, GA 31098-1635

1.1. **Background/Scope**:

There will be three subtasks associated with the Performance Work Statement (PWS): Subtask 1 will be for HQ AFRC Reserve Network Support; Subtask 2 will be for the Global Command Control System (GCCS); and Subtask 3 will be other administrative, program management, project management, staff, and subject matter expert (SME) support. This task order will require labor at Headquarters Air Force Reserve Command (HQ AFRC) and multiple locations. ~~**(See Table 4.)**~~

For the Reserve Network Support service objectives include management of desktops, servers, networks, and related functional services. The contractor shall perform Information Technology (IT) Operations and Maintenance (O&M) and Logistics; Program Management; Systems Engineering; and Training of the IT Infrastructure. In coordination with the Local Accountable Officer (AO) and Headquarters Air Force Reserve Command, Director of Communications (HQ AFRC/A6), the contractor shall provide organizational support services which include: Telecommunications Support; Plans, Programs, Projects, services; Communications Systems Maintenance; Operate Network Control Centers (NCCs)/Communication Focal Points (CFPs) including Network Administration, Network Management, and Messaging Services. Provide Video Teleconference (VTC) services, Information Assurance (IA), web administration, and training services. The Contractor shall provide services to maintain the designated sites in an operational status by supporting all fielded command, control and network support systems.

For the GCCS, vendor is responsible for the operation of SIPRNET core services. Service objectives include: management, administration, and user Help Desk support for the information technology environment at HQ AFRC, and other local and remote AFRC sites. This support is centralized at HQ AFRC and supports AFRC host and tenant locations.

For other administrative support services, objectives include resource planning and management for the development and implementation of organizational concepts, operations concepts, and integration of functional roles and missions, action officer, subject matter experts, and technical advisors. Support shall include programmatic reviews and formulation, budget management, manpower management and advice, and future mission roles. Products/deliverables shall be in the form of, but are not solely limited to, position descriptions, technical reports, organizational structures, summaries, and formal and informal briefings. This support will be at HQ AFRC, Robins AFB GA.

Any and all Full Time Equivalent (FTE) information identified in this PWS or its attachments is provided to aid offerors in developing their quotes in response to this performance-based acquisition and represent the Government's estimated workload based on historical information for planning purposes only and is not intended to be binding on either party or to be the only possible solution to the requirement. Contractors should quote adequate contractor personnel to ensure full and successful compliance with the PWS for the life of this order.

1.2. The tasks to be accomplished by this Performance Work Statement are divided into three (3) subtasks. Each subtask will have labor (firm fixed price or FFP). In addition, time and materials (T&M) CLINs are required in order to support real-world and mission impact issues, as they arise. All contractor requests for either overtime and/or comp time must be preapproved by the government Contracting Officer Representative (COR) or CO <u>BEFORE</u> the said overtime/comp time is performed.

1.3. **<u>Program Management</u>**. The contractor shall identify an On-Site Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program Management Reviews and ensuring all standards referenced herein are adhered to. The On-Site Project Manager shall be able to respond to Robins AFB, GA within 2 hours. The On-Site Project Manager shall:

- Be an experienced and responsible individual accustomed to liaison activity with management-level activities of the Department of Defense (DoD).
- Be responsible for the actions necessary to ensure efficient program management
- Be delegated the necessary authority to make on-site decisions to include:
    - Control over vendor personnel utilization and hours expended and authorization of material and travel expenditures. Ensure COR and CO is informed of ALL decisions that will impact costs (up or down) and service delivery impacts.
    - Must have at least 3 years <u>documented</u> experience handling or managing workforce of over 75 people at multiple locations.

1.3.1. <u>Network User Licensing Program</u>. Military, civilian and contract personnel must all meet the same licensing requirements before access is permitted to network resources [as outlined in Air Force Instruction (AFI) 33-115, Vol II], *Licensing Network Users and Certifying Network Professionals*. The Accountable Officer (AO) at each location will sign off on the completion of the required certification verification and will notify the COR once this has been accomplished. A quarterly update of status is part of the information that will be submitted to the COR each month by email to ensure contractor service is satisfactory.

1.3.2. <u>Network Professional Certification Program</u>. Contract personnel shall be evaluated using a combination of written evaluation and performance based demonstrations in accordance with (IAW) AFI 33-115, Vol II. Contractors requiring elevated network administrative rights (estimated at approximately 85) will have to comply with the Department of Defense Directive (DODD) 8570.1, *Information Assurance Training, Certification and Workforce Improvement*

Plan, (aka 8570) certification process prior to working on this task order. Furthermore, all contractors requiring elevated network administrative rights shall be required to maintain 8570 certification at all times as well as complete the Privileged Access Agreement (PAA) form.

1.4. **Program Support**:

1.4.1. The contractor shall provide program management support to ensure that the requirements of this task order are accomplished. An "in person" task kick-off meeting at Robins AFB, is required within seven calendar of the date of award.

1.4.2. The contractor shall participate in programmatic meetings, reviews, and briefings associated with this task order.

1.4.3. The contractor shall submit a trip report for any travel performed in support of the task. This report shall be electronically delivered to the COR via the General Service Administration (GSA) IT Solutions Shop (ITSS) web-based Order Processing System.

1.4.4. The contractor shall identify and report all program management actions in a Monthly Technical Summary (MTS) Report and/or as requested by the Government. This report shall be electronically delivered to the COR via the GSA ITSS web-based Order Processing System and contain the following information:

- Brief description of requirements.
- Brief summary of accomplishments during the reporting period and significant events regarding the task order.
- Any current or anticipated problems and the resolution.
- Summary of all major events and other pertinent information.
- Technical user support activity summary.
- Summary of associated travel completed.
- Summary of planned travel.
- Brief summary of activity planned for the next reporting period.
- Task schedules/work plans.
- Task performance metrics.
- Task software quality metrics.

1.4.5. The contractor shall identify and report financial management status in a Monthly Financial Summary (MFS) Report. This report shall be electronically delivered to the COR via the GSA ITSS web-based Order Processing System and contain the following information:

- Charges [broken out for labor, training, travel, other direct costs (ODC), Contractor Access Fees (CAF)] during the reporting period.
- Billing summary broken out by labor and travel including deferred charges.
- Staffing history.
- Vendor T&M Expense/Burn Rates.

SUBTASK 1 – AFRC USER NETWORK SUPPORT – NETWORK SUPPORT NATIONWIDE

2.0. PROJECT BACKGROUND. Headquarters, Air Force Reserve Command (AFRC), Robins Air Force Base (AFB), GA is responsible for the operation, management, administration, and user support for the information technology environment at AFRC, and other sites ~~referenced in Table 4~~. Currently AFRC is undertaking three major software conversions—a server consolidation, a network operating system conversion from Microsoft Windows 2000/2003 to Server 2008, and traditional Major Command (MAJCOM) centric network and network services shall continue their present consolidation phase into the AFNET, Joint Information Enterprise (JIE) or other, as directed. It is envisioned that network and core services consolidation will generally reduce workload in this task over the task order life. Workload will transition to support of enterprise architecture with Service Oriented Architecture (SOA) tools (etc., warehousing, enterprise service business, "mashup" (see para 5.27. for definition), business analytics, dashboard implementation.

Support is required to maintain, enhance, and improve the sites in an operational status by supporting all fielded network support systems, and projects/tasks required by the Government on NIPRNET and SIPRNET. The Government base support may include other tenants.

The major systems include but are not limited to:

- The Air Mobility Command (AMC) Command and Control Information Processing System (C2IPS).
- The Air Combat Command (ACC) Contingency Theater Automated Planning System (CTAPS).
- The Global Command and Control System (GCCS).
- The Air Force Mission Support System (AFMSS).
- The Global Command Support System (GCSS).
  Other Command and Control (C2) systems as required by the Command, Control, Communications, Computers and Intelligence (C4I) architecture.
- Global Decision Support System (GDSS).
- Patriot Excalibur (PEX).
- Financial Management (FM) Systems.
- Standard Procurement System (SPS).
- Supply Asset Tracking System (SATS).
- Defense Biometric Identification System (DBIDS).
- Joint Environment Toolkit (JET) (weather system).

Note: Not all systems listed above are present at each location. Supported applications are intended to be representative and are not all inclusive.

The major activities being performed include but are not limited to:

- Exchange/MS Outlook/mobile computing.
- SharePoint.

- Enterprise/Base network infrastructure.
- File system/storage/backup/restore.
- Printer and print server management.
- The Global Command Support System (GCSS).
- CFP/NCC.
- User account management.
- MS Office.
- Network/system monitoring.
- Vulnerability Management.
- Remote access management (i.e., MS ISA/TMG).
- Virtual suite management.
- Maintenance Tasking Order (MTO)/Time Compliance Notification Order (TCNO)/Time Compliance Technical Order (TCTO) compliance/reporting.
- Directory services.
- Enterprise Architecture SOA Implementation.
- Voice Over Internet Protocol (VOIP)/Everything Over Internet Protocol (EOIP).
- Unified communications [including Microsoft Communications Server (OCS), Lync, and DCO].

Note: Not all activities listed above are present at each location. Supported activities are intended to be representative and are not all inclusive.

2.1. **Task Specific FIP/Networking Environment**:

The AFRC network environment consists of approximately 12 Local Area Networks (LANs), 850 servers and 20,000 workstations at multiple buildings and sites. At AFRC, about 2,000 workstations are networked to share peripherals, communications and facilities infrastructure, and about 25 PCs stand alone.

Systems are government owned-server based systems using approved Windows Workstation Operating Systems and approved Microsoft server Operating Systems. The configuration will change during the course of the task as sites move toward standardized Commercial Off-the Shelf (COTS) software and hardware to complete the open system architecture. It is anticipated that during this task order, that a migration from a Windows XP/Vista/7 platforms (SDC 1.x, 2.x, and 3.x) for all systems will occur and migration to Windows 8 (SDC 4.x) and potentially new OSs. It is also anticipated that an elimination of Windows Server 2003 (and prior OSs) and migration to Server 2012 and newer server OSs will occur. Vendors should plan accordingly.

2.2. **Network Environment**. HQ AFRC is spread out in approximately nine (9) buildings on Robins AFB. Buildings are connected to the primary headquarters building (210) via fiber optic cable.

The government has separate sources to maintain the hardware infrastructure and repair equipment. However, the contractor shall do minor repairs such as board swapping and equipment resets. Any parts/materials required will be provided by the Government. In addition, the contractor is responsible to contact appropriate government and/or commercial agencies to resolve maintenance problems. The contractor is required to inventory upon arrival/acceptance, remove, pack and ship equipment (actual shipping costs will be paid for by the Government, vendor is required to make item(s) ready to be shipped and deliver as necessary to the shipping point) components and once received, replace and/or connect these repaired components into their appropriate systems:

AFRC uses the following list of standard equipment and COTS software, which will be the primary focus of the task. Non-standard software and hardware will be secondary. Additional brands of equipment and software could be procured during this task order period and will also be covered. The government has a separate contractor to maintain the hardware infrastructure.

2.2.1. Hardware:

Network Servers
Routers
Wireless Access Points
Network Switches
Dell
Cisco
SAN/NAS Storage Systems
Windows Desktop & Laptop PCs
Tape back-up systems
UPS
HP-UX
EMC

2.2.2. Software:

MS Office Suite (2007, 2010, 2013)
Microsoft Exchange
Network Browsers (Microsoft Internet Explorer, FireFox/Mozilla)
SQL 2005/2007/2012
Pure Edge
SharePoint
MIBS/SMB
NFS and SMB
OCS/Lync/DCO
Remedy Management System (RMS)
Microsoft BackOffice
Oracle
HP Net Management
Windows Active Directory
MS SCCM
ISA/TMG/F5
Third Party software as required
PowerShell

2.3. Operating Systems:

CISCO IOS
F5
Windows operating systems including:
Windows Vista, Win 7, & Win 8
Windows Server 2003, 2008, & 2012

*Others as required by Government – to updating of the Operating Systems and an on-going effort to keep up with the latest updates.

2.3. HQ AFRC Support. The chart below illustrates the logical structure of HQ support within this subtask to better understand the following requirements.

HQ AFRC Support (at Robins)
AFNet Support Element (ASE) – (See para 2.3.1. thru 2.3.1.7.)
MAJCOM Support Element (MSE) – (See para 2.3.2. thru 2.3.2.10.)
Communications Focal Point (CFP) – (See para 2.3.3.)

The first HQ organizational construct is the AFNet Support Element (ASE). The ASE assists the AFNet organizations manage AFRC's (and potentially other MAJCOMs AFNet hardware, software, and services (core and non-core). The ASE utilizes Remedy (or replacement) to document IT issues/activities/fix actions for users as well as maintenance activities on the infrastructure, servers, services, etc. Additionally, the ASE participates in meetings, conferences, telecons, VTCs, etc. to maintain relationships with the AFNet organizations especially with the Enterprise Service Units (ESUs), the Enterprise Service Desk (ESD), and ASE and ESU back shops, the base CFPs and technicians, the local HQ CFP, and the HQ MAJCOM Support Element (MSE). The ASE technicians achieve/maintain the proper 8570 certifications as required by the AFNet. ASE technicians must be trained and evaluated by position as required by Air Force Instructions (AFIs) and the AFNet policies and procedures. Approximately 8 FTE's.

The ASE executes the following functions (but not limited to): directory services, messaging (e.g., Exchange, Outlook Web Access (OWA), Hub transport servers, Client Access Server (CAS), Blackberry, Good, etc.), monitoring (e.g., SMARTS, NetIQ, NetCop, NetCool, System Center Operations Manager (SCOM), etc.), virtual management (e.g., VMWare, Hyper-V, etc.), ticket management/routing/queuing technician workload via Remedy/email, Virtual Private Network (VPN) capabilities/server management (e.g., Microsoft ISA, TMG, etc.), Dynamic Host Control Protocol (DHCP) server/IP address management, file storage management/technician activities, backup management/activities and other activities as required. The ASE operates these core services on NIPRNET and SIPRNET.

The second HQ organizational construct is the MAJCOM Support Element (MSE). The MSE works command-wide, enterprise approaches/activities for IT support. The MSE provides command management, configuration, oversight, technical knowledge and management of enterprise functions such as printer server management (etc., work command printer policies, configuration issues, etc.), user blackberry/Good/IOS activities (e.g., add and delete users on the Blackberry Enterprise Server (BES), track licenses usage, determine active/stale user usage, etc.), command-wide Remedy (or replacement) ticket views (to include HQ and the bases/locations), provide assistance to the local/AFRC base CFP and ASE to facilitate support efforts for users with the AFNet, other agencies, SharePoint support, command LRA support, and miscellaneous server support. The MSE provides, updates, maintains, posts content, creates content (in addition to receiving content from others (ASE, CFP, etc.) for the command's Tier 0 site via SharePoint. The MSE technicians will achieve/maintain the proper 8570 certifications as required by AFNET/DISA. Approximately 9 FTE's.

The third HQ organizational construct is the local HQ CFP. The HQ CFP works base-level type activities for the HQ AFRC campus. This includes, but not limited to, touch labor for workstation, printer, or other hardware/software issues that requires a physical presence of a technician or an effort not supported by the AFNet. HQ CFP technicians may be required to reside at alternate HQ AFRC campus locations at the discretion of mission requirements. Additionally, the CFP technicians work any patching requirements, mobile computing device issues requiring touch labor/scripting, OCS Live Meeting/DCO/Lync support, local printer management and security configuration, Remedy (or replacement) ticket management, updates, tracking, routing, etc., and Standard Desktop Configuration (SDC) imaging. The CFP technicians also maintain proficiency in current technological trends, operating systems, SDC imaging capabilities/ requirements, troubleshooting, achieve and maintain 8570 certifications, etc. Approximately 12 FTE's.

All technicians engaged in working on IT equipment (e.g., servers, workstations, etc...) or working user IT issues will use the Air Force IT trouble ticketing system (currently Remedy) to document those activities/efforts.

All technicians responsible for IT equipment (e.g. servers, workstations, etc.) will complete vulnerability management activities to include patching, configuring, documenting, reporting, (and other related activities as directed by the government) these activities in the appropriate/designated systems [e.g., ACT, (to be replaced by Continuous Monitoring and Risk Scoring (CMRS) system VMS, Remedy, etc...]. The contractor must maintain vulnerability management standards ~~status~~ on all NIPR/SIPR servers/workstations that meets Defense Information Systems Agency (DISA) and/or Air Force (AF) standards. Compliance standards will be whichever is more restrictive. AFRC/SC provides scanning services and metrics open vulnerabilities and server administrators, as required, to support the vulnerability management process.

2.3.1. **AFNet Support Element [SC/ASE] – (Robins AFB, GA ONLY)**. The primary function of the ASE is to be an extension of the Air Force Network's (AFNet) Enterprise Service Units (ESU). Currently, the functions that exist in the ESU (and therefore the ASE) are Messaging, Directory Services, Monitoring, File/Storage, Virtual Management, collaboration services, and Crew/Event Operations. Except for the potential changes in ASE-level messaging, these activities may change but the overall functions are expected to stay relatively static during the term of this task order (NIPRNET/SIPRNET).

General ASE Task Support:

- Performs on-site Local and Wide Area Network (LAN/WAN) security management functions.
- Assists with system administration functions.
- User account maintenance/support.
- File and account maintenance.
- System/File recoveries.
- System builds/rebuilds/imaging.
- Implementation of system management procedures.
- Technical assistance and support of file servers to include communications processors; LAN/WAN components.
- Determines network node configuration.
- Supports backups for functional servers in the infrastructure.
- Software configuration management.
- Software and hardware upgrades and revisions.

- Systems analysis to resolve configuration and equipment problems.
- Provides recommendation to return sites to an operational status.
- Troubleshoots hardware, software and network problems.
- Software and hardware maintenance, patches, and tech refresh installs, as directed.
- Attends government called In-Progress Reviews (IPRs), technical meetings, and briefings in support of the command and control and network support systems.
- Coordinates, as technical liaison, technical requirements with the government Technical Point of Contact (TPOC).
- Reports volumes, resolutions times, and other information identified by the local AO on the Monthly Status Reports. The Government CFP software may be able to provide data for reporting.

2.3.1.1. **Messaging [SC/SE] (1 FTEs)**. The tasks required:

- Works with the government leadership as the focal point for problem resolution and is the primary point of contact for problems relating to AFNet issues and AFNet user issues on Microsoft Exchange, Blackberry, Good, Hub Transport Servers, Client Access Servers, ISA/TMG, Outlook Web Access (OWA), Outlook Anywhere, and other miscellaneous servers/services within the AFNet's Messaging team responsibilities.
- Coordinates with HQ/base Client Support Technicians (CSTs), or CSTs for physical resolution, as required.
- Executes tasks as coordinated with ESU on day-to-day support/maintenance activities on the servers and services.
- Coordinates with appropriate agency to ensure backups and monitoring is being accomplished.
- Coordinates, documents, test, validates, and deploys new technology, as required.
- Provides physical server support, as required.
- Utilizes Remedy to document, coordinate, route, resolve, and close user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, and close server/services tickets.
- Achieves and maintains 8570 certification requirements.
- Maintains proficiency and knowledge on latest technological efforts
- Conducts/assists with installs/configurations of the hardware and software for appropriate servers to Air Force specifications.
- Installs, configures, operates, and maintains network messaging applications.
- Must be proficient in performing Microsoft (MS) Exchange E-mail system administration.
- Maintains accuracy of the Global Address List (GAL) as well as local Address Lists.
- Troubleshoots wide area mail flow.
- Implements change requests approved by AFNet configuration management processes

2.3.1.2. **Directory Services [SC/ASE] (1 FTE)**. The tasks required:

- Works with the government leadership as the focal point for problem resolution and is the primary point of contact for problems relating to AFNet issues and AFNet user issues on Microsoft Active Directory (AD), Dynamic Host Control Protocol (DHCP), Domain Name Service (DNS) and Group Policy Object (GPO).

- Coordinates with HQ/base CFPs, or CSTs for physical resolution, as required.
- Executes tasks as coordinated with ESU on day-to-day support/maintenance activities on the servers and services.
- Coordinates with appropriate agency to ensure backups and monitoring is being accomplished.
- Coordinates, documents, tests, validates, and deploys new technology, as required.
- Provides physical server support, as required.
- Utilizes Remedy to document, coordinate, route, resolve, and close user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, close server/services tickets.
- Have knowledge of PowerShell.
- Achieves and maintains 8570 certification requirements.
- Conducts/assists with installs/configurations of the hardware and software for appropriate servers to Air Force Specifications.
- Maintains proficiency and knowledge on latest technological efforts.
- Performs preventive maintenance and ensures data recovery capability through proper data backup scheduling and execution.

2.3.1.3. **Server/Infrastructure Monitoring Configuration [SC/ASE] (2 FTEs)**. The tasks required:

- Works with the government leadership as the focal point for problem resolution and is the primary point of contact for problems relating to AFNet issues and AFNet user issues relating monitoring of servers, infrastructure, services, etc.
- Coordinates with server/services owners on monitoring devices, servers and services and the respective thresholds.
- Ensures server/service owners and the operational team receives their respective alerts accurately; modify as required.
- Coordinates with HQ/base CFPs, or CSTs for physical resolution, as required.
- Executes tasks as coordinated with ESU on day-to-day support/maintenance activities on the servers and services.
- Coordinates with appropriate agency to ensure backups and monitoring is being accomplished.
- Coordinates, documents, tests, validates, and deploys new technology, as required.
- Provide physical server support, as required.
- Utilizes Remedy to document, coordinate, route, resolve, and close user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, close server/services tickets.
- Achieves and maintains 8570 certification requirements.
- Maintains proficiency and knowledge on latest technological efforts (current tools are SMARTS, NetIQ/App Manager, NetCop, NetCool, SCOM, etc.).
- Conducts/assists with installs/configurations of the hardware and software for appropriate servers to Air Force specifications.

2.3.1.4. **Enterprise File/Storage [SC/ASE] (1 FTE).** The tasks required:

- Manages NIPRNET and SIPRNET capabilities across the command.
- Works with the government leadership as the focal point for problem resolution and is the primary point of contact for problems relating to AFNet issues and AFNet user issues on file storage, backup, restoration, etc.
- Coordinates with HQ/base CFPs, or CSTs for physical resolution, as required.
- Executes tasks as coordinated with ESU on day-to-day support/maintenance activities on the servers and services.
- Coordinates with appropriate agency to ensure backups and monitoring is being accomplished.
- Coordinates, documents, tests, validates, and deploys new technology, as required.
- Provides physical server support, as required.
- Utilizes Remedy to document, coordinate, route, resolve, and close user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, close server/services tickets.
- Achieves and maintains 8570 certification requirements.
- Maintains proficiency and knowledge on latest technological efforts.
- Works with users and organizations to standardized file storage directory structures.
- Actively monitors, updates, and corrects file/storage access permissions.
- Monitors and conducts file/storage backups and restores.
- Coordinates with messages (et al) to monitor and execute core and non-core servers and services restores (including user email restores).
- Conducts/assists with installs/configurations of the hardware and software for appropriate servers to Air Force specifications.

2.3.1.5. **Virtual Management [SC/ASE] (1 FTE).** The tasks required:

- Works with the government leadership as the focal point for problem resolution and is a primary point of contact for problems relating to AFNet issues and AFNet user issues on virtual suite management/maintenance.
- Coordinates with HQ/base CFPs, or CSTs for physical resolution, as required.
- Executes tasks as coordinated with ESU, INE, ASE, MSE, MCCC, CFP, AFRC bases, etc… on day-to-day support/maintenance activities on the servers and services.
- Coordinates with appropriate agency to ensure backups and monitoring is being accomplished.
- Coordinates, documents, tests, validates, and deploys new technology, as required.
- Provides physical server support, as required.
- Utilizes Remedy to document, coordinate, route, resolve, and close user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, close server/services tickets.
- Achieves and maintains 8570 certification requirements.
- Maintains proficiency and knowledge on latest technological efforts, to include VMWare, Hyper-V, and PowerShell.

- Conducts/assists with installs/configurations of the hardware and software for appropriate servers to Air Force specifications.
- Must be able to travel and assist AFRC bases in virtual management issues, installs, projects, etc.

2.3.1.6. **ASE Activity Leader [SC/ASE] (1 FTEs).** The tasks required:

- Responsible for oversight of ASE backshops.
- In conjunction with the government lead, is the ASE team leader/director.
- As required, attends meetings, conferences, leadership forums with government and non-government organizations.
- Regularly visits and briefs AFNet organizations that the ASE supports and interacts with.
- Corresponds/coordinates at all levels--with technicians and leadership inside AFRC, AFNet operational organizations and staff organizations such as an Air Force Space Command (AFSPC), Air Force Network Integration Center (AFNIC), 24th Air Force (24 AF).
- Provides leadership, management and mentorship to the ASE team; manages workload, coordinates with AFNet regarding tasks, tickets and issues.
- Coordinates with HQ, AFRC bases, AFRC tenants, and other MAJCOMs for AFNet support and coordinating ASE support to those organizations.
- Leads and directs ASE tasks on day-to-day support/maintenance activities for the ASE and follows through on expanding the ASE role in the AFNet.
- Coordinates with appropriate ESU, Integrated Network Operations Security Center (INOSC) or other external agencies, as required, to ensure AFNet issues are being resolved.
- Coordinates with agencies to ensure ASE documents, tests, validates, and deploys new technology, as required.
- Directs ASE team members to utilize Remedy to document, coordinate, route, resolve, and close user issues.
- Ensures ASE technicians correctly utilize Remedy in the execution of ASE duties resolving user and server issues.
- Achieve and maintain 8570 certification requirements, as required.
- Maintain proficiency and knowledge on latest technological efforts.

2.3.1.7. **Enterprise Service Controller [SC/ASE] (1 FTEs).** The tasks required:

- Works with the ASE Team Leader and government leadership as the focal point for problem resolution and is the primary point of contact (POC) for problems relating to AFNet issues and AFNet user issues that are in the purview of the ASE.
- Coordinates with HQ/base CFPs, or CSTs for physical resolution, as required.
- Executes tasks as directed by the ASE team leader as well as those coordinated with the ESU on support, maintenance, and user activities for the ASE.
- Coordinates with appropriate ASE team members, ESD, ESU, INOSC or other external agencies, as required, to ensure user issues are being resolved.

- Establishes a metrics program to document, trend, perform analyses, and brief the ASE and AFNet performance.
- Coordinates with to ensure ASE documents, tests, validates, and deploys new technology as required.
- Coordinates physical server support, as required.
- Utilizes Remedy to open document, coordinate, route, resolve, and close user issues. Ensures ASE technicians correctly utilize Remedy in the execution of ASE duties resolving user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, close server/services tickets.
- Ensures ASE technicians correctly utilize Remedy in the execution of ASE duties resolving server and services issues.
- Achieves and maintains 8570 certification requirements, as required.
- Maintains proficiency and knowledge on latest technological efforts.

2.3.2. **MAJCOM Support Element [SC/MSE] – (Robins AFB, GA ONLY)**. The primary function of the MSE is to be the AFRC enterprise IT support activity. The functions planned for the MSE are command-wide maintenance/support and planning/execution services to include, but not limited to, print and print server management, Blackberry Enterprise Server (BES) user application management, Good user application management, SharePoint support, FAX server, Internet Protocol Television (IPTV) support, file/storage/backup activities, collaboration capabilities (including ~~and~~ Office Communication Server (OCS) and Lync), and supporting miscellaneous servers (NIPNET and SIPRNET).

General Task Support:

- Performs on-site Local and Wide Area Network (LAN/WAN) security management functions.
- Assists with certification and accreditation.
- Assists with on-site system administration functions.
- User account maintenance/support.
- File and account maintenance.
- System/File recoveries.
- System builds/rebuilds/imaging.
- Implementation of system management procedures.
- Technical assistance and support of file servers to include communications processors; workstations; and LAN/WAN components.
- Determines network node configuration.
- Supports backups.
- Software configuration management.
- Software and hardware upgrades and revisions.
- Systems analysis to resolve configuration and equipment problems.
- Provides recommendation to return sites to an operational status.
- Troubleshoots hardware, software and network problems.
- Software and hardware maintenance, patches, and tech refresh installs, as directed.
- Assists with front-end, end-user CFP functions to local site users.

- Attends government called In-Progress Reviews (IPRs), technical meetings, and briefings in support of the command and control and network support systems.
- Coordinates, as technical liaison, technical requirements with the government Technical Point of Contact (TPOC).
- Reports volumes, resolutions times, and other information identified by the local AO on the Monthly Status Reports. The government CFP software may be able to provide data for reporting.

2.3.2.1. Reserved

2.3.2.2. **AFRC Wide Area/COOP File Server Storage [SC/MSE] – (March ARB, CA and Robins AFB, GA – 2 FTEs--1 FTE at each location)**. The tasks required:

Primary Requirements:

- Command Focal Point for problem resolution on EMC Storage File Server Consolidation devices and Interim Continuity of Operations Capability (I-COOP) backup monitoring and replication issues.
- Works closely with the AFRC Storage Manager on all aspects of storage system interoperability.
- Attends meeting in support of command related functions, technical meetings, and briefings concerning storage and storage management.
- Performs systems analysis to resolve configuration and equipment problems. Creates and reports metrics when requested.
- Works with AFRC Base NCC/CFPs to schedule hardware and software maintenance and updates to the storage equipment at each location.
- Schedules and executes backups, tests, and monitors successful backup replication and recovery operations to ensure successful and optimum performance of data recovery and backup capability.
- Initially populates file share data to I-COOP locations either by tape and/or other mechanical means or by full data transfer from all AFRC bases.
- Provides telephone CFP support for all aspects of the I-COOP File Server Consolidation to include; share creation on the devices, privileges to file share areas, allocation of file share space on base devices.
- Monitors storage devices for backup success, recovery success, capacity planning, and recommends expansion of devices as need arises.
- Assures application licenses are updated and prevents unlicensed software from being used on the network.
- Builds servers to support storage monitoring tools.
- In the event of data loss to an AFRC base or bases, would be responsible for re-establishing file data loss at the effected location and support to again regain normal operating conditions at the effected base.
- Assists in new installs of file storage equipment.
- Coordinates base repair for Base NCC/CFP storage hardware and software, initial installs, routine maintenance, and upgrades.

- Some travel may be associated with this position at the direction of the government representative.

Secondary Requirement:

- Oversees day-to-day back-up operations of CommVault software at all AFRC locations.
- Provides backup support for CommVault software operations.
- Provides support for tape and disk to disk backup systems.
- Knowledge of hardware and software:
  - Microsoft File Server configuration according to AF Standards.
  - EMC Control Center.
  - EMC Celerra Replicator.
  - EMC Celerra.
  - EMC Centera.
  - Quantum Tape library.
  - CommVault backup software.
  - CommNet Software.
  - CommVault Data Migrator.

2.3.2.3. **Infrastructure Engineer/Technician/Internet Services [SC/MSE] – (Robins AFB, GA ONLY – 2 FTEs)**. The tasks required:

- Assists the government in configuring and maintaining routers and switches comprising the WAN/LAN backbone.
- Expert knowledge of VOIP/Voice Over Secure Internet Protocol (VOSIP).
- Maintains the Network Management System (NMS) including system backups.
- Monitors Internet Protocol address space through utilization of DHCP or static configuration.
- AFRC engineering leadership for IP space management.
- Assists with the infrastructure engineering for the AFRC LAN/WAN architecture.
- Assists with the technology tech refresh/management for the command.
- Assists the COR in directing the infrastructure technicians at HQ and base level for issues, questions, engineering issues, maintenance problems.
- Makes recommendations to the Government for infrastructure upgrades, configurations, efforts at HQ and bases.
- Manages local domain name service information when necessary.
- Configures user accounts.
- Monitors security of the devices and implement new configurations and/or IOS upgrades, as required.
- High TDY requirement due to base level support.
- Expert knowledge of TACLANES and Cisco.

2.3.2.4. **Print Management [SC/MSE] – (Robins AFB, GA ONLY – 1 FTE).** The tasks required:

- Makes recommendations for implementing the command's efforts for overall AFRC print server policies and management.
- Plans and implements enterprise print server management, security, configuration control for AFRC's AFNet print servers.
- Makes recommendations on new printer technology for devices, management software/ processes, configuration controls and methods.
- Implements policies across the command for new printer device selection.
- Coordinates with bases and HQ CFP on print server application management. If required, will maintain base printer servers.
- Assists the COR as the Command technical lead on printer server and device technology.
- Coordinates on process improvements to make better efficiencies in AFRC to save resources (etc., costs, personnel, etc.).
- Coordinates with ASE on print server support for the AFNet print servers located at HQ and bases across the command.
- Have knowledge of print servers as well as PowerShell.

2.3.2.5. **Blackberry Enterprise Server (BES) and Good User Application Management [SC/MSE] – (Robins AFB, GA ONLY – 1 FTE)**. The tasks required:

- Makes recommendations for the command's efforts for overall AFRC Blackberry and Good policies and management.
- Supports Blackberry, Android, Apple devices, and other devices/capabilities AFRC pursues.
- Assists the COR with implementing enterprise Blackberry/Good device management, security, configuration control for AFRC's mobile user community.
- Makes recommendations on new mobile technology for devices, management software/processes, configuration controls and methods.
- Makes recommendations on implementing policies across the command for new mobile device selection/implementation.
- Assists the COR as the Command technical lead on Blackberry and Good server and device technology.
- Makes recommendations on process improvements to make better efficiencies in AFRC to save resources (etc., costs, personnel, etc.).
- Makes recommendations to ASE on BES and Good server (Good Dynamix) support for the AFNet BES and Good servers.
- Makes recommendations to ASE on issues arising that might impact the mobile computing environment (etc., BES server upgrades).
- Assists the COR in tracking BES user license usage. Gathers data to determine best use of licenses, stale license usage, etc.
- Makes recommendations with HQ and bases to ensure BES usage accurate and validates users on the BES are current.
- Other tasks as required.

2.3.2.6. **User Issue-AFNet Resolution Specialist [SC/MSE] – (Robins AFB, GA ONLY – 1 FTE).** The tasks required:

- Makes recommendations for implementing the command's efforts for overall user-AFNet issue coordination, advocacy, and resolution.
- Assists in coordinating and resolving specific issues regarding credential issues such as status changes for Air Reserve Technicians (ARTs), Active-Guard Reserve (AGR), users with multiple roles in the AFNet.
- Assists the COR in reading, developing, improving, and distributing AFNet Standard Operating Processes (SOPs).
- Assists the COR in submitting changes to the AFNet for SOPs, checklists, etc. to improve AFNet activities.
- Assists in searching Remedy tickets across the command (HQ and bases) for credentialing (as an example) for issues requiring MAJCOM advocacy to resolve.
- Makes recommendations to ASE, MCCC and ESD to resolve issues.
- Assists the COR in developing Tier 0 content to improve user community on issues.
- Provides recommendations to local technicians and base level technicians on issues.
- Provides recommendations to bases on user ticket resolution, as required.
- Provides recommendations on process improvements to make better efficiencies in AFRC to save resources (etc., costs, personnel, etc.).
- Other tasks, as required.
- Have knowledge of Remedy.

2.3.2.7. **HQ MAJCOM LRA [SC/MSE] (Robins AFB GA ONLY – 1 FTE)**. Manage request and delivery of Alternate Tokens for base users requiring Alt Token credentials (both NIPR and SIPR). Alternate Tokens provide hardware credentials for network authentication in lieu of Common Access Card (CAC) or name/password. Process for Alt Token issuance will be governed by Air Force Public key Infrastructure (PKI) System Program Office. One person is required at HQ AFRC with base level support of this task (the description below is for the HQ support contractor).

- Performs as the HQ AFRC Local Registration Authority (LRA) to include issuing software certificates to support organizational email and admin accounts.
- Provides LRA leadership to the base LRA.
- Interfaces with AFNet organizations and Air Force Directory Services (AFDS) (and others) to resolve issues.
- Works and supports PKI-related requests/tasks (e.g., certificates on organizational email accounts).
- Performs as the AFRC MAJCOM LRA to issue smart card tokens Secure Internet Protocol Router Network (SIPRNET).
- Understands networking and PKI principles.
- Maintains an LRA database. Includes, as required, installing, upgrading and configuring hardware/software used to support the database; performing system/database backups.

- Works with Remedy to work many (not all) of the activities regarding certificates and admin accounts.
- Supports AFRC bases and tenants, as required, with support and TDY to facilitate/work issues.

2.3.2.8 **AFRC Installation Warning System (IWS) Alerts Emergency Management System – [A6X/MSE] [Robins AFB, GA ONLY – 1 FTE].** Support the AFRC Installation Warning System (IWS) Alerts Emergency Management System and provide support to approximately 76,000 AFRC personnel who are using the IWS alerts software. Duty hours of the IWS help desk support are projected from 0800-1630 Eastern Standard Time (EST), Monday thru Friday. The contractor shall be responsible for resetting Wing Operator/Administrator passwords, responding to trouble calls from AFRC Wings (42) and working trouble resolution issues with the appropriate Wing and/or ATHOC Help Desk. The Contractor shall assist users in generating reports and queries to assist in tracking alert status, and in future training of AFRC personnel in the use of IWS Alerts (estimated at 6 classes/year training 10 people per class). Problems and issues not resolvable by their office shall be elevated to the ATHOC Help Desk, and/or appropriate ATHOC Engineer. Work center personnel shall also be responsible for troubleshooting the IWS Alerts system with ATHOC engineers and working with end users and HQ AFRC Director of Communications Plans and Policy Program Manager (HQ AFRC/A6XP) to resolve any problems detected.

2.3.2.8.1. Contractor shall be responsible for supporting the IWS Alerts server (2 databases and 6 application servers) located at Robins and Dobbins. Additionally, the contractor is responsible for patching, upgrading, backing up servers, responding to tasking orders from AFRC and/or the AFNet (etc., Network Tasking Orders). The frequency of these tasks range from executing backups daily (as an example) to responding as required.

2.3.2.8.2. Temporary Duty (TDY)/travel to Dobbins may be required once a month to do such things as server backup, managing the backup servers, patch management, etc. for these activities that could not be completed remotely.

2.3.2.8.3. Performance Locations. **~~See Table 4 – Locations and Types of Service.~~**

AFRC – Robins AFB, GA
ARPC – Buckley AFB, CO
Pentagon – Washington D.C.
301 AW – NAS JRB Ft Worth (Carswell JRB), TX
304 RS – Portland IAP, OR
434 AW – Grissom ARB, IN
439 AW – Westover ARB, MA
~~440 AW – Pope AFB, NC~~
919 CS – Duke Field, FL
452 AW – March ARB, CA
482 AW – Homestead ARB, FL
910 AW – Youngstown ARB, OH
911 AW – Pittsburgh ARS, PA

2.3.2.9. **General Server/Services Support – [SC Robins AFB, GA ONLY] (1/2 FTE)**:

Task Required: General Server Maintenance and Support:

- Acts as command Internet Protocol Television (IPTV) Technician and command FAX Server Technician.
- Makes recommendations on implementing the command's efforts for overall AFRC IPTV policies, management and support.
- Assists with implementing enterprise IPTV management, security, configuration control.
- Coordinates, tests, documents, evaluates and implements new IPTV technology.
- Assists the COR as the Command technical lead on IPTV.
- Makes recommendations on process improvements to make better efficiencies for IPTV in AFRC to save resources (e.g., costs, personnel, etc.).
- Makes recommendations on implementing the command's efforts for overall AFRC FAX server, policies, management and support.
- Assists with implementing enterprise FAX server management, security, configuration control.
- Coordinates, tests, documents, evaluates and implements new FAX technology.
- Assists the COR as the Command technical lead on FAX server.
- Makes recommendations on process improvements to make better efficiencies for FAX services in AFRC to save resources (e.g., costs, personnel, etc.).
- Assists with certification and accreditation.
- Assists with on-site system administration functions.
- User account maintenance/support.
- File and account maintenance.
- System/File recoveries.
- System builds/rebuilds/imaging.
- Implementation of system management procedures.
- Technical assistance and support of file servers to include communications processors; workstations; and LAN/WAN components.
- Determines network node configuration.
- Supports backups.
- Software configuration management.
- Software and hardware upgrades and revisions.
- Systems analysis to resolve configuration and equipment problems.
- Provides recommendation to return sites to an operational status.
- Troubleshoots hardware, software and network problems.
- Software and hardware maintenance, patches, and tech refresh installs, as directed.
- Assists with front-end, end-user CFP functions to local site users.
- Attends government called In-Progress Reviews (IPRs), technical meetings, and briefings in support of the command and control and network support systems.
- Coordinates, as technical liaison, technical requirements with the government TPOC.

- Reports volumes, resolutions times, and other information identified by the local AO on the Monthly Status Reports. The government CFP software may be able to provide data for reporting.
- Have working knowledge of server operating systems.

2.3.2.10. **Vulnerability Management Server/Workstation Support – [SC Robins AFB, GA ONLY] (1 FTE).** The vulnerability management activity requires one highly skilled technician supporting critical, MAJCOM-wide security-based functions that are required to always be resourced. Task Required:

- Establishes scripts, plans and execution strategies to meet the approximately 40 Cyber tasking orders.
- Establishes scripts, plans and execution strategies to meet the approximately 345K vulnerabilities across the 23K workstations and 800 servers in AFRC.
- Plans, develops, executes, reports, and tracks server and workstation vulnerabilities for the command.
- Develops documents and executes scripts to patch servers and workstations.
- Educates and facilitates vulnerability management with PMO and non-PMO system owners to include sharing and executing (if requested) patching scripts.
- Designs and executes other methods, as required, to facilitate vulnerability management.

2.3.3. **Communications Focal Point (CFP) [SC/CFP] – (Robins AFB, GA ONLY – 12 FTEs)**. The tasks required:

- Assists the COR as the focal point for problem resolution and is the primary point of contact for problems (coordinates with CSTs for physical resolution, as required).
- Uses a central repository for technical advice and solutions for network systems, (CST/CFP drive, Tier 0, etc.), software applications assistance, automatic data processing support, hardware exchange, and repair service support.
- Assists with reporting network performance metrics using Remedy Action Reporting System.
- Utilizes Remedy to enter, document, track, coordinate, route, resolve, and close user ticket issues.
- May be required to visit other locations to resolve minor hardware/software/network malfunctions.
- Coordinates with ESD, MSE, ASE, ESU, and MCCC to work all user issues.
- Works with HQ software license manager to prevent unlicensed software from being used on the network.
- Images/reimages/work-assist tech refresh for workstations (e.g., laptops, desktops, tablets, etc.), printer support, hand-held mobile devices, etc.
- Supports HQ OCS user capabilities and OCS Live Meeting usage.
- Assists in evaluation, testing, documenting, deploying new user-base technology.
- Be assigned as and function as an equipment custodian, as needed.
- Assists with local user training, perform initial fault assessment and resolution.

- Assists in working, coordinating, documenting, resolving, and closing trouble tickets when tasked and coordinate activities with Client Support Technicians (CSTs).
- Manages the AFNet Remedy queues located at and/or supporting the base/users.
- HQ level support will include those IAO duties as required by AFNet.
- Utilizes Remedy Management System (RMS) or similar service, maintain historical database of reported problems, and associated events, provide the local AO with statistics of calls received, number of trouble tickets submitted, average resolution time, listing of technical bulletins and information guides issued, and trend analysis information.
- Tier 1 and 2 support includes support to NIPR/SIPR services.
- Has a working knowledge of Remedy and scripting.

2.3.3.1. Reserved

2.4. Base Support:

The Network Control Center (NCC) and the Communication Focal Point (CFP) are distinct but work very closely together to ensure the base mission is accomplished as required via IT. The focus of each is different but they coordinate continuously to ensure user issues are resolved effectively.

The NCC is the base organization responsible for the data center, servers, routers and switches.

The CFP is the base organization that supports the user community, their workstations and manages base-level Remedy tickets.

All technicians engaged in working on IT equipment (e.g., servers, workstations, etc...) or working user IT issues will use the Air Force IT trouble ticketing system (currently Remedy) to document those activities/efforts.

All technicians responsible for IT equipment (e.g. servers, workstations, etc.) will complete vulnerability management activities to include patching, configuring, documenting, reporting, (and other related activities as directed by the government) these activities in the appropriate/designated systems (e.g., ACT, VMS, Remedy, etc...). The contractor must maintain a vulnerability management status on all NIPR/SIPR servers/workstations that meets AFRC, DISA and/or AF standards. AFRC/SC provides scanning services and metrics open vulnerabilities and server administrators, as required, to support the vulnerability management process.

{Note: Modification **011** ~~**09**~~ ~~**will**~~ **removes** all support services provided at Pope AFB, **NC** under this task order**,** ~~**if the modification is exercised**~~**.}**

Base Support (at each base)
Network Control Center (NCC) – (See Section 2.4.1.)
Communications Focal Point (CFP) – (See Section 2.4.2.)
Base-Level LRA – (See Section 2.4.3.)

2.4.1. **Network Control Center (NCC) [All Bases]**. The base NCC is focused more on the infrastructure and servers/services and controls the physical operations and security of the network for the site. Additionally, the NCC personnel will assist the CFP in solving individual user issues, as required. NCC duties include LAN administration, Network configuration, infrastructure management (servers, switches, routers, wireless infrastructure, NCC UPS/power systems, and NCC security and operations).

- Network backbone management (hardware, software and servers).
- Network access (login, file and print servers, web access).
- Network Security.
- Hosting Functional Servers.
- Works in Remedy to document all network activities.
- Perform on-site Local and Wide Area Network (LAN/WAN) security management functions.
- Assists with certification and accreditation.
- Assists with on-site system administration functions.
- User account maintenance/support.
- File and account maintenance, as required.
- Coordinates/performs server/file recoveries.
- Server/infrastructure builds/rebuilds/imaging.
- Implementation of system management procedures.
- Determines network node configuration.
- Supports backups for functional servers in the infrastructure.
- Software configuration management.
- Software and hardware upgrades and revisions.
- Systems analysis to resolve configuration and equipment problems.
- Provides recommendation to return sites to an operational status.
- Troubleshoots hardware, software and network problems.
- Software and hardware maintenance, patches, and tech refresh installs, as directed.
- Attends government called In-Progress Reviews (IPRs), technical meetings, and briefings in support of the command and control and network support systems.
- Coordinate, as technical liaison, technical requirements with the government Technical Point of Contact (TPOC).
- Reports volumes, resolutions times, and other information identified by the local Accountable Officer (AO) on the Monthly Status Reports. The government software may be able to provide data for reporting.
- Performs initial fault assessment and resolution.
- Works, coordinates, documents, resolves, and closes trouble tickets when tasked and coordinate activities with CSTs/CFP.
- Utilizes Remedy Management System (RMS) or similar service, maintain historical database of reported problems, and associated events, provide the local AO with statistics of calls received, number of trouble tickets submitted, average resolution time, listing of technical bulletins and information guides issued, and trend analysis information.
- Prepares and coordinates with user and the government, reports of software, operational, or documentation deficiencies.

- TACLANE rekeying/programing, as required.
- Complies with any/all applicable AF standards and procedures as well as subsequent releases (i.e., TO 00-33A-1001, AFI 33-115, etc.).
- Has a working knowledge of scripting and Cisco OSs.
- Achieves and maintains 8570 certification requirements.

2.4.2. **Communication Focal Point (CFP) [All Bases].** The CFP is the single focal point at each site listed in the attachment table to work/support user-based issues for the site. Currently, the AFNET's Enterprise Service Desk (ESD) is the entry point for users with IT issues. However, the local CFP is the users' entry point for many issues other than Enterprise IT Issues. Additionally, the ESD is reducing its capability and that reduced support is being absorbed by the CFP. It is expected that during the term of this task order, DOD will execute some consolidation efforts (e.g., JIE) that may or may not reverse the workload being sent to the bases. The CFP facilitates the following core services to all site users:

- Network access (login, file and print services, web access).
- OCS Live Meeting support.
- Mobile computing device issues requiring touch labor.
- Workstation security (e.g., patching).
- Workstation software install/troubleshooting (e.g., email).
- Ticket lifecycle management.
- User account maintenance/support.
- Maintains proficiency in current technological trends, operating systems.
- Achieves and maintains 8570 certifications, etc.
- File and account maintenance.
- Workstation file/profile recoveries.
- Workstation/SDC builds/rebuilds/imaging.
- Assists in software configuration management.
- Software and hardware upgrades and revisions.
- Assists in system analysis to resolve configuration and equipment problems.
- Provides recommendation to return sites to an operational status.
- Troubleshoots hardware, software and network problems.
- Software and hardware maintenance, patches, and tech refresh installs, as directed.
- Liaison for support of unresolved network system trouble calls by working with other service desks. (Information on all help desks for all systems will be provided by the Government.)
- Attends government called IPRs, technical meetings, and briefings in support of the command and control and network support systems.
- Coordinates, as technical liaison, technical requirements with the Government TPOC.
- Reports volumes, resolutions times, and other information identified by the local AO on the Monthly Status Reports. The government CFP software may be able to provide data for reporting.
- Assists with local user training and training assistances, perform initial fault assessment and resolution. Assist in working, coordinating, documenting, resolving, and closing trouble tickets when tasked and coordinate activities with CSTs.

- Manages the AFNet Remedy queues located at and/or supporting the base/users.
- Base level support will include those tasks required by the AFNet related to user support as Information Assurance Officers (IAOs), as tasked.
- Utilizes RMS or similar service, maintain historical database of reported problems, and associated events, provide the local AO with statistics of calls received, number of trouble tickets submitted, average resolution time, listing of technical bulletins and information guides issued, and trend analysis information.
- Prepares and coordinates with user and the government, reports of software, operational, or documentation deficiencies.
- Complies with any/all applicable AF standards and procedures as well as subsequent releases (i.e., TO 00-33A-1001, AFI 33-115, etc.).
- Has a working knowledge of Remedy and scripting.

2.4.3. **Base-Level LRA [All Bases] (½ FTE)**. Manage request and delivery of Alternate Tokens for base users requiring Alt Token credentials. Alternate Tokens provide hardware credentials for network authentication in lieu of Common Access Card (CAC). Process for Alt Token issuance will be governed by Air Force PKI System Program Office. Base level support of this task:

- Performs as the Local Registration Authority (LRA) to include issuing software certificates to support organizational email and admin accounts.
- Understands networking and PKI principles.
- Maintains an LRA database; includes, as required, installing, upgrading and configuring hardware/software used to support the database; performing system/database backups.
- Works with Remedy to work many (not all) of the activities regarding certificates and admin accounts.
- During the task order period, the Government anticipates implementation of SIPR hardware tokens.

2.5. HQ SME Support:

There are a few SMEs located at the HQ that facilitate headquarters support.

HQ SME Support
Telephone – Homestead – (See Section 2.5.1.)
Telephone – ARPC (Buckley) – (See Section 2.5.2.)
VTC/Presentation Support – (See Section 2.5.3.)
SharePoint – (See Section 2.5.4. thru 2.5.5.)
MAJCOM SOCE – (See Section 2.5.6.)

2.5.1. **Telephone and Communications – [Homestead AFB, FL ONLY] (2 FTEs)**. The Contractor shall provide Organizational Support to enable the effective and efficient Telecommunications, Communications and Information (C&I), and selected Communications and Computer Systems maintenance and support to each site.

- Provides day-to-day operation and maintenance for the new cables and telephone switch being installed. Personnel shall have inside/outside plant experience, switch programming and maintenance.
- Provides training for contractor assigned technician to support new and/or upgraded equipment in the event of a telephone system upgrade.

2.5.1.1. Telecommunications Support. The Contractor shall provide the following telecommunications support IAW Allied Communications Publication (ACP) 134, *Telephone Switchboard Operating Procedures*, AFI 33-111, *Voice Systems Management*, and as described below.

2.5.1.2. Telephone Operations:

- Operates and sustains local, long distance, and Defense Switch Network (DSN) telephone service in accordance with AFI 33-111, with and without operator assistance, by configuring, operating and maintaining the telephone switch for an estimated customer base of 4300 users.
- Maintains 911 capabilities.
- Performs hardware, software, and firmware installations on the switch.
- Performs backup and restore activities.
- Provides voice mail administration services and maintains the telephone database.
- Ensures that all switch maintenance is provided by switch manufacturer-certified personnel.
- Attaches technical exhibits for each base describe required switchboard support and activities and service operating hours.
- Performs trouble ticket correction for all telecommunication-related issues.
- Assists in the implementation for all current and future telecommunication requirements to include the telephone switch and its related peripherals.
- Assists in management, addition, and discontinuous for base circuit actions.

2.5.1.3. Local Service. The Contractor shall maintain outgoing service to the local area for all authorized subscribers who make official calls in direct support of the mission.

2.5.1.4. Defense Switch Network (DSN). The current DSN service must not be altered without prior approval of local cognizant management officials and GSA Acquisition Contracting Officer (ACO).

2.5.1.5. Long Distance Service. The Contractor shall maintain commercial long distance service for authorized users of the telephone service IAW AFI 33-111. This does not include incoming collect calls. Exceptions to this procedure will be determined and approved by the local Wing/Base commanders who establish policy regarding collect phone calls.

2.5.1.6. Telephone Switch. The Contractor shall maintain the telephone switch and associated components in good working order to meet mission requirements. Actions in support of this effort such as identifying and obtaining (at government expense) materiel, equipment, supplies, technical assistance, and other ancillary support are the Contractor's responsibility. Material, equipment and supplies will be purchased by the government for installation by the contractor.

2.5.1.7. Conference Calls. The Contractor shall maintain conference call capability and support conference call requirements, when requested.

2.5.1.8. Base Cable Plant. The Contractor shall manage the base cable plant. Responsibilities include but are not limited to:

- At government expense, maintains the base government-owned cable plant, locate and mark buried cable, interact with the 38th Engineering Installation Group (38 EIG) at Tinker AFB to assist in maintaining base cable plant drawings.
- Interacts with 38 EIG Systems Telecommunications Engineering Manager (STEM) to assist in the modernization of the base cable plant through planning, implementation, and documentation of base cable plant requirements into base communication blueprint.
- Coordinates emergency repairs to the cable plant.
- Facilitates site surveys. These site surveys will be at Homestead where the contractor shall physically go to each building to ensure that the telephones are working.

2.5.1.9. Inside Distribution. Contractor shall operate and maintain all existing inside building (cable and equipment) distribution (telephonic and LAN). Responsibilities include but are not limited to:

- Minor repairs to inside building cabling.
- Trouble shooting and diagnostics.
- Equipment swap outs.
- Coordinates on new construction inside building distribution.

2.5.1.10. Telephone Maintenance:

- Establishes a "help-desk" function for receiving reports of telephone/circuit troubles.
- Takes action needed to restore the telephone service within the performance parameters established by this PWS.

2.5.1.11. Tracking of System Status:

- Uses the Remedy system to track and report status of the telephone system.
- Reviews the status of the system on a continuing basis to ensure that the system operates properly and is available to meet mission requirements.
- Promptly initiates corrective action on deficiencies identified within the system.
- Notifies the responsible government authority within 30 minutes of any outages affecting more than 10 people.
- Informs Government management officials on the status of the system, including plans and timelines to correct known deficiencies.
- Provides monthly metrics regarding the status of phone systems.

2.5.1.12. Access to and training on Telephone Switch for Training of Government Personnel:

- Provides access to and training on the telephone switch for Government personnel (Traditional Reservists). The Government will provide verification to the Contractor that such Government personnel are properly authorized to operate the switch before the Contractor is required to grant access.
- Takes appropriate precautions to safeguard any materials made available to Government personnel during these training periods. The Contractor must be notified in advance to allow the Contractor to adjust schedules to support the Government's training needs.

2.5.2. **Telephone and Communications – [HQ ARPC, Buckley AFB, CO] (2 FTEs)**. The Contractor shall provide organizational support to enable the effective and efficient Telecommunications, Communications and Information (C&I), and selected Communications and Computer Systems maintenance and support.

2.5.2.1. The Contractor shall provide Voice Over Internet Protocol (VOIP) and network support to enable the effective and efficient transport of telecommunications and data information over ARPC's LAN Network. The contractor should be able to operate, upgrade, maintain, diagnose and repair the following systems: Cisco Unified Communication Manager, Cisco Call Center, Unity Voice Mail system and network LAN components to include but not limited to switches for access/distribution/core layers, routers and other ancillary equipment used to support communications requirements for Headquarters, Air Reserve Personnel Center (HQ ARPC) (i.e., TFTP/DHCP/servers). Contractor should be well versed with Audio Codec's, Power over Ethernet (POE), Session Initiated Protocol (SIP), subnetting, Virtual LAN (VLAN), Spanning Tree Protocol (STP), Quality of Service (QOS), and routing protocols. Additionally, the contractor should be able to operate, upgrade, maintain, diagnose and repair communication circuits that enter and traverse the ARPC facility. These include, but are not limited to, the Integrated Services Digital Network (ISDN) T1 trunking between ARPC phone system and Host base telephone system providing ARPC's access to local, long distance, and DSN telephone service. To effectively achieve the desired results, the contractor shall provide equipment programming, planning, project management, and perform a full range of technical and system management/administration functional tasks in support of the fielded Network Support systems as required by applicable AFIs/guidance which will be provided to the contractor. The contractor is required to comply with and execute tasks received in network tasking/compliance orders and security directives. The contractor shall perform the tasks IAW issued work orders. The tasks listed are illustrative in the general task scope.

2.5.2.2. General Task Scope. Examples of on-site systems operation functions, as required:

- Performs on-site LAN security management functions.
- Assists with certification and accreditation.
- Assists with on-site system administration functions.
- User account manager.
- File and account maintenance.
- System recoveries.

- System builds.
- Implementation of system management procedures.
- Technical assistance and support of file servers to include mail servers and support equipment; communications processors; workstations; and LAN components.
- Determines network node configuration.
- Software configuration management.
- Software and hardware upgrades and revisions.
- Systems analysis to resolve configuration and equipment problems.
- Provides recommendation to return sites to an operational status.
- Troubleshoots hardware, software and network problems.
- Software and hardware maintenance, patches, and tech refresh installs, as directed.
- Assists with front-end, end-user help desk function to local site users.
- Liaison for support of unresolved C2 and network system trouble calls by working with each systems regional service desk. (Information on all help desks for all systems will be provided by the government).
- Attends government called IPRs, technical meetings, and briefings in support of the command and control and network support systems.
- Provides minutes to the government of IPRs and technical meetings. Minutes and trip reports from the meeting or conferences shall be provided to the government representative within five (5) duty days of return from trip.
- Coordinates, as technical liaison, technical requirements with the government TPOC.
- Reports volumes, resolutions times, and other information identified by the local Accountable Officer (AO) on the Monthly Status Reports. The government Help Desk software may be able to provide data for reporting.
- Maintains E911 capabilities through documentation and reporting in accordance to host base procedures.
- Performs hardware, software, and firmware installations on servers, gateways and end instruments that make up the Unified Communications and Call Center systems.
- In conjunction with Network staff, provides and maintains network QOS with diagnostic utilities, test equipment and protocol analyzers.
- Provision end instruments IAW Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs), and Unified Communications Resource documents.
- Achieves and maintains 8570 training requirements.
- Performs backup and restore activities.
- Provides voice mail administration services and maintain the telephone database.

2.5.2.3. Defense Switched Network (DSN). The current DSN service must not be altered without prior approval of local cognizant management officials and GSA ACO.

2.5.2.4. Long Distance Service. The Contractor must maintain commercial long distance service for authorized users of the telephone service in accordance with AFI 33-111. This does not include incoming collect calls. Exceptions to this procedure will be determined and approved by the local commanders who establish policy regarding collect phone calls.

2.5.2.5. Inside Distribution. Contractor must operate and maintain all existing inside Building 444 (cable and equipment) distribution (telephonic and LAN). Responsibilities include but are not limited to:

- Minor repair to inside building cabling.
- Trouble shooting and diagnostics.
- Equipment swap outs.
- Coordinates on new construction inside building distribution.

2.5.2.6. Telephone Maintenance. The Contractor must take whatever action necessary to restore the telephone service in the event of a malfunction. The contractor must provide for the Add, Moves, and changes, system administration, help-desk functions for receiving reports of telephone/circuit troubles and telephone operator function. Due to limited system configuration documentation, the Government recommends some of the vendor's technical personnel have current system experience for easy transition of services.

2.5.2.7. Telephone Control Officer (TCO). The Contractor must perform the TCO function for the bases and must train unit TCOs IAW AFI 33-111.

2.5.2.8. Tracking of System Status:

- Uses the Remedy system to track and report status of the telephone system.
- Reviews the status of the system on a continuing basis to ensure that the system operates properly and is available to meet mission requirements.
- Promptly initiates corrective action on deficiencies identified within the system.
- Notifies the responsible government authority within 30 minutes of any outages affecting more than 10 people.
- Informs Government management officials on the status of the system, including plans and timelines to correct known deficiencies.
- Provides monthly metrics ~~statistics~~ regarding the status of phone systems.

2.5.3. **Video Teleconferencing – [SC Robins AFB, ONLY]** ~~**(See Table 4)**~~. The HQ AFRC VTC environment consists of 11 VTC suites using ISDN connectivity. **The HQ AFRC VTC environment consists of 11 VTC suites using ISDN connectivity (approx).** On a weekly basis, approximately 20-40 VTC sessions and 100-125 conference room events occur. During this contract, VTC suites will migrate to IP connectivity and will integrate with various unified command solutions. Additionally, the VTC hub located at HQ AFRC will provide VTC hosting services to AFRC, AFRC host bases, and tenants expanding local support to users throughout the command. Host base and tenant support will be provided as much as possible within current manning levels and work hours. Administrative oversight of the VTC positions is in AFRC/SCOS.

2.5.3.1. **VTC Operations Center System Engineer (1 FTE)**. The tasks required:

- Video Teleconferencing (VTC) hub manager for VTC hub (located at HQ AFRC) supporting VTC session hosting for all AFRC locations.

- Schedules, coordinates and facilitates VTC requests/sessions.
- Maintain VTC Account Database.
- Tracks, documents and briefs management on VTC utilization trends.
- Maintains and updates web-based VTC schedule.
- Provides access list for room supporting VTC hub infrastructure equipment.
- Provides maintenance and/or troubleshooting support for legacy ISDN issues affecting VTC hub services.
- Maintains Inventory control, track suspense~~’~~s, issue notices.
- Provides daily VTC availability reports to appropriated agencies.
- Provides installation support, technical documentation, ongoing troubleshooting and maintenance, and on-site training support for VTC services.
- Act as centralized VTC network maintenance focal point, receives and responds to alerts from VTC users/network VTC systems.
- Conducts basic troubleshooting, and coordinates with appropriate vendors for maintenance support.
- Configures systems, communications devices, and peripheral equipment.
- Provides centralized VTC network support through Tandberg web-based client-server architecture.
- Develops and maintains AFRC VTC Directory.
- Installs, configures, and upgrades network hardware/software.
- Sets up VTC sessions, to include bridging of VTC calls as needed through configuration and management of network bridges.
- Maintains network bridges to support VTC sessions.
- Develops training materials, and train on-site personnel in the proper use of the VTC-Audio/Visual (A/V) hardware/software.
- Supports on-site installations from maintenance vendor, configures the hardware and software for the appropriate telecommunications service, and test for connectivity and interoperability.
- Makes reservations with DVSG, GVS, or other networks as needed, and coordinates with each base on their VTC availability.
- Conducts site~~s~~ surveys at Robins AFB; assess and document current site configuration.
- Be familiar with various A/V technologies.
- Be familiar with VTC technologies and common architecture equipment (i.e., Cisco, Codian).
- Builds specialized interconnecting cables.
- Displays experience with multicast on desktops (streaming audio/video), audio conferencing, point-to-point, and multipoint video conferencing.
- Achieves and maintains 8570 certification requirements.
- Performs safe custodian duties.
- Manages secure key material for classified VTC equipment.

2.5.3.2. **VTC Operations Center Senior VTC Administrator (1 FTE)**. The contractor shall provide Senior-level support to the VTC Engineer in the following areas:

- VTC configuration manager and facilitator for HQ AFRC.

- Schedules, coordinates, facilitate, and set up VTC requests/sessions.
- Maintain VTC Account Database utilizing Tandberg Management Software.
- Tracks, documents and briefs management on VTC utilization trends.
- Maintains and updates web-based VTC schedule.
- Maintains inventory control, track suspense's, issue notices.
- Provides daily VTC non-availability reports to local government AO for this service.
- Provides installation support, technical documentation, ongoing troubleshooting and maintenance, and on-site training support for desktop VTC services.
- Acts as centralized VTC network maintenance focal point, receive and respond to alerts from VTC users/network VTC systems.
- Conducts basic troubleshooting, and coordinate with appropriate vendors for maintenance support.
- Configures systems, communications devices, and peripheral equipment.
- Provide centralized VTC network support through Tandberg Management Software web-based client-server architecture.
- Develops and maintains AFRC VTC Directory.
- Maintains network bridges to support VTC sessions.
- Develops training materials, and trains on-site personnel in the proper use of the VTC-A/V hardware/software.
- Performs on-site installations, configures the hardware and software for the appropriate telecommunications service, and test for connectivity and interoperability.
- Makes reservations with DVSG, FTS2001, or other networks as needed, and coordinate with each base on their VTC availability.
- Conducts site~~s~~ surveys; assesses, and documents current site configuration and user requirements.
- Builds specialized interconnecting cables.
- Displays experience with multicast on desktops (streaming audio/video), audio conferencing, point-to-point, and multipoint video conferencing.

2.5.3.3. **VTC Operations Center Presentation Support Manager – [SC Robins AFB, GA and Homestead ARB, FL ONLY] (4 FTE at Robins and 1 FTE at Homestead)**. The contractor shall perform the following duties:

- Schedules, coordinates, facilitates, and sets up VTC requests/sessions.
- Provides Senior-level presentation support for HQ AFRC VTC-enabled conference rooms.
- Coordinates presentation requirements for conference room users, presents PowerPoint and/or other presentation support through use of multimedia systems in these rooms.
- Provides technical support to customers on presentation capabilities and requirements for the conference rooms.
- Assists in scheduling of rooms for presentation support.
- Assists with setup of VTC call sessions on HQ AFRC VTC hub.
- Conducts basic trouble shooting, and coordinates with VTC Operations Chief on any issues which require resolution.
- Configures systems, multimedia devices and peripheral equipment.

- Must be familiar with various AV technologies and software.
- Supports on-site maintenance from vendors.

2.5.3.4. **<u>HQ USAF/RE VTC Facilitator/Web Developer – [Pentagon ONLY] (1 FTE)</u>**.

- Provides video conferencing and web development support to Headquarters United States Air Force, Office of Reserve Affairs (HQ USAF/RE). Serves as VTC configuration manager, web developer, and facilitator for HQ USAF/RE.
- Schedules, coordinates, facilitates, and sets up VTC requests/sessions.
- Maintains VTC account information.
- Coordinates funding and VTC utilization for HQ USAF/RE customers.
- Tracks, documents, and briefs management on VTC utilization trends.
- Maintains and updates web-based VTC schedule.
- Maintains inventory control, track suspense's, issue notices.
- Provides daily VTC availability reports to appropriated agencies.
- Provides installation support, technical documentation, ongoing troubleshooting and maintenance, and on-site training support for desktop VTC services.
- Acts as centralized VTC network maintenance focal point for the HQ USAF/RE VTC system, receive and respond to alerts from VTC users/network VTC systems.
- Conducts basic troubleshooting, and coordinate with HQ AFRC VTC Operations for maintenance support. Configure VTC systems, related communications devices, and peripheral equipment.
- Provides centralized VTC network support through Tandberg Management Software web-based client-server architecture.
- Installs, configures, and upgrades network hardware/software.
- Sets up VTC sessions, to include bridging of VTC calls through the AFRC VTC Operations Office at Robins AFB, GA.
- Develops training materials, and train on-site personnel in the proper use of the VTC-A/V hardware/ software.
- Performs on-site installations, configure the hardware and software for the appropriate telecommunications service, and test for connectivity and interoperability.
- Makes reservations with DVSG, FTS2001, or other networks as needed, and coordinate with bases on their VTC availability.
- Analyzes existing requirements and prepare specifications for hardware/software acquisitions and/or upgrades.
- Be familiar with various A/V technologies including taping, editing, and special effects such as graphics, post production, and duplication.
- Builds specialized interconnecting cables.
- Display experience with multicast on desktops (streaming audio/video), audio conferencing, point-to-point, and multipoint video conferencing.
- Provides HQ USAF/RE web support.
- Designs and develop portal interface web pages as needed.
- Duties also include Presentation Support as required.

2.5.4. **<u>Senior SharePoint Administrator – [SC Robins AFB, GA ONLY] (1 FTE)</u>**. The tasks required:

- Responsible for the development, planning, design, testing, implementation, upgrade, and management of internal and external SharePoint sites (includes 2010, 2013 and future upgrades) supporting AFRC and its partners.
- Functions include, determining overall website design and structure, monitoring web site functionality, security, and integrity, troubleshooting and resolving problems, reviewing, testing, collecting and analyzing website statistics, evaluating new web applications and providing technical advice to web content providers.
- Provides expert knowledge of SharePoint Architecture and functionality and a strong working knowledge of related technologies such as: Windows Server administration, Windows Architecture, SQL Server 20xx, Internet Information Server, Active Directory, Secure Socket Layer (SSL), Kerberos, ISA and Microsoft Office desktop application integration with SharePoint.
- Experiences with workflow and InfoPath integration with other technologies, is necessary.
- Achieves and maintains 8570 certification requirements.
- Analyzes AFRC's information architecture, understand MAJCOM, Base and Wing departmental requirements, to configure and maintain organizational taxonomies, site collections, policies, procedures, and solutions.
- Works closely with developers to install, debug, and maintain necessary code of assigned software.
- Stays current with present trends and activities.
- Must have strong communication, customer service, troubleshooting, and organizational skills and the ability to complete assigned work with minimal instruction and supervision.
- Experience. Require at least 2 years of SharePoint 2010/2013 admin experience and 3 years Microsoft Office SharePoint Server (MOSS) 2007 experience.

2.5.5. **<u>SharePoint Administrator – [SC Robins AFB, GA ONLY] (1 FTE)</u>**. The tasks required:

- Works with the Senior SharePoint Administrator as the focal point for problem resolution and is the primary point of contact for problems relating to SharePoint servers and services.
- Performs physical resolution of user issues, as required.
- Executes day-to-day support/maintenance activities on the servers and services.
- Coordinates with appropriate agency to ensure backups and monitoring is being accomplished.
- Coordinates, documents, tests, validates, and deploys new technology, as required.
- Provides physical server support as required.
- Utilizes Remedy to document, coordinate, route, resolve, and close user issues.
- Utilizes Remedy to open, document, coordinate, route, resolve, close server/services tickets.
- Achieves and maintains 8570 certification requirements.

- Conducts/assists with installs/configurations of the hardware and software for appropriate servers to Air Force specifications.
- Maintains proficiency and knowledge on latest technological efforts.
- Performs preventive maintenance and ensures data recovery capability through proper data backup scheduling and execution.
- Coordinates with user/customer community for content and site structures.
- Troubleshoots issues with SharePoint as well as issues with content delivery, site usage, etc.
- Requires critical thinking, logic, and attention to detail.
- Performs well under pressure in a fast-paced production.
- Supports the project staff, IT, and developments teams as well other users that will integrate and or interact with the SharePoint environments.
- Facilitates the gathering and documentation of requirements from users to facilitate design.
- Assists in the set-up of global standards and controls for internal team and project sites and assist in the development of training for business users on SharePoint functionality.

2.5.6. **<u>MAJCOM Service Oriented Cloud Environment (SOCE) and Sustain Team [SC] (5 FTE)</u>**:

2.5.6.1. The task requires:

- Coordinates with A6 staff, customers, programmers, and contractors to ensure proper Enterprise SOCE Tools implementation and operations.
- Tracks status of Certification and Accreditation (C&A), prior to SOCE implementation.
- Ensures funding is addressed and advocated for by the customer.
- Ensures SOCE projects are completed on time.
- Responsible for identifying any Personally Identifiable Information (PII) issues and proper protection of SOCE data.
- Works to support life-cycle SOCE requirements.
- Manage projects to support the planning, scheduling and implementation of Enterprise Architecture Tools throughout their life-cycle within the command.
- Develops documentation (project plans, implementation plans, etc.,); maintaining program/project folders for all SOCE.
- Coordinates with AFRC/A6O enterprise Architecture, the AFRC/Chief Technology Officer, and AFRC/A6X Requirements.
- TDY may be required to attend program and/or project meetings; to meet with AFRC or Air Force functional planners to work implementation and/or support issues.

2.5.6.2. **<u>SOCE Capability</u>**. There are four related capability areas in which AFRC has identified gaps that need to be filled. These program goals areas are:

2.5.6.2.1. Provide loose coupling so that various presentation services (e.g., SharePoint, etc.) are not tightly bound to various data sources that will be presented (usually within dashboards, but potentially within other types of web apps). This capability is intended to provide faster time-to-market and more efficient sustainment of presentation services. This requirement is best satisfied by procuring, configuring, and sustaining an Enterprise Service Bus (ESB), as well as the Service Oriented Architecture (SOA) IT infrastructure, and implementing best practices, governance structure, and security posture required to support that ESB. Government will procure hardware and software in support of this task, requirement is for labor supporting installation, operation, management and sustainment of the capability.

2.5.6.2.2. Providing advanced and predictive analytics so that various models of AFRC readiness, force management and surge capability, recruitment, and other AFRC areas can be automated as part of an overall strategic decision support initiative. The Government envisions that this requirement is best satisfied by procuring, configuring, modeling, and sustaining both an Operational Data Store (ODS) and a Data Warehouse (DW) that support automated multi-dimensional storage of AFRC mission models, which in turn provide a platform on which highly performing analytics processing is to be done.

2.5.6.2.3. Providing a rapid and on-demand data aggregation capability, so that emergent mission requirements that entail the correlation of multiple authoritative and operational data sources can be achieved with little or no technical knowledge on the part of the owner of the tasker requiring that data correlation. The Government envisions that this requirement is best satisfied by procuring, configuring, managing, and sustaining a “Mashup” Service.

2.5.6.2.4. Provide professional services to support technical solutions, and an IT platform supporting these services, so that measurable Analysis of Alternatives (AoA) can be produced for potential solutions satisfying the above three capability areas: This requirement is best satisfied by obtaining the professional services of staff that has demonstrated hands-on development, configuration, modeling, and architecting in each of the three other capability domains listed above.

Figure 1 below describes our notional architecture to provide the capabilities described.

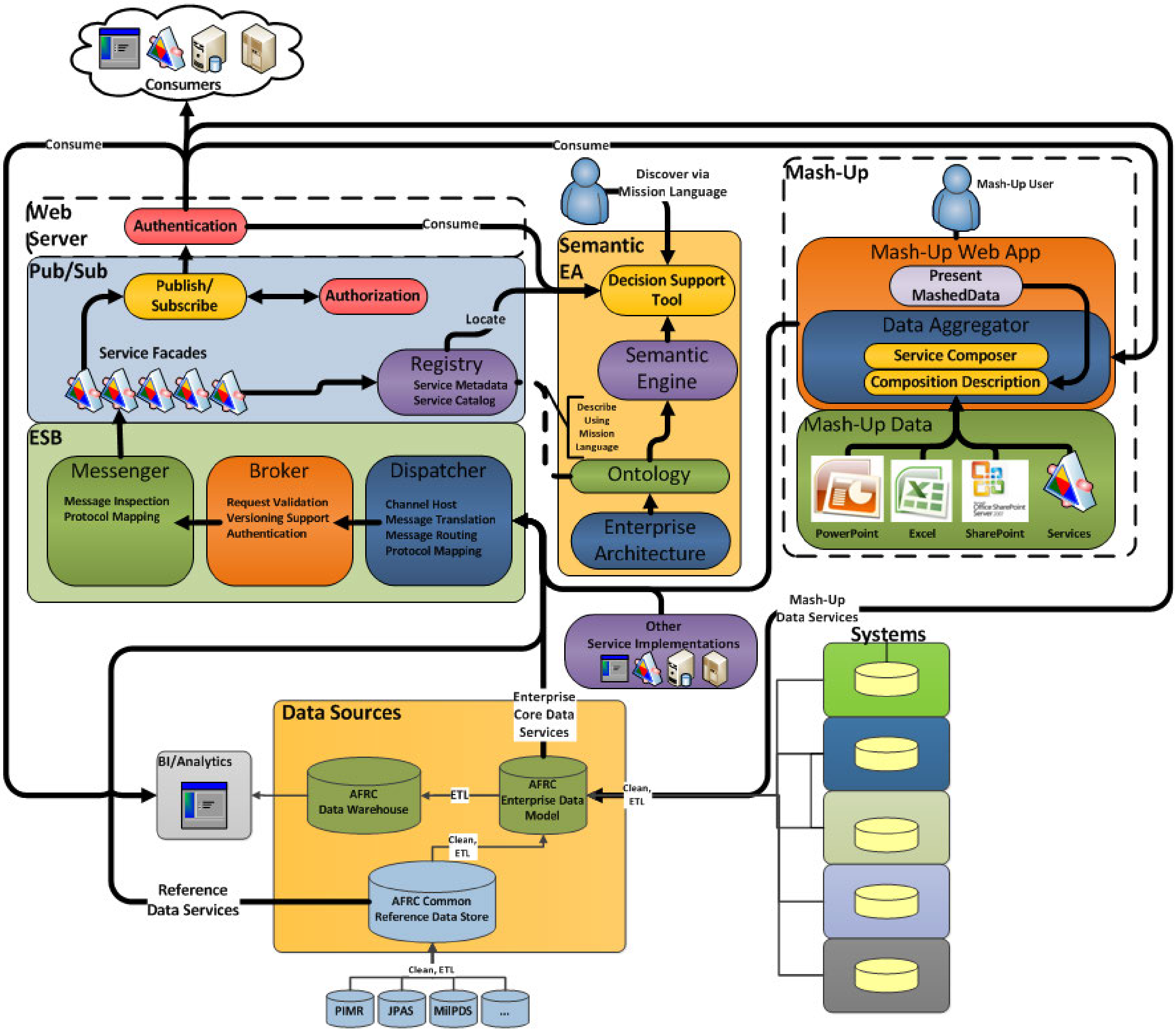

Figure 1. Notional Architecture

2.5.6.3. Description of SOCE Tools**:**

2.5.6.3.1. Enterprise Service Bus Description: A commercial product based AFRC Enterprise Service Bus (ESB) platform is required to implement a service-oriented architecture. The ESB provides loosely coupled connections between services and data sources enabling data sharing and data pull automation. The ESB will serve as AFRC's Service Oriented Cloud Environment (SOCE) platform and will be employed in SOCE data exchanges by other government and industry partners, as deemed necessary by the Government.

2.5.6.3.1.1. Current State**.** AFRC has configured a 64 bit version of BizTalk which provides an interim ESB capability. It consumes services from two AFRC systems, ARCNet and AFRISS-R (Air Force Recruiting Information Support System –Reserve), to display readiness and accessions data. This is an initial attempt to automate AFRC Strategic Plan metrics using SOA principles.

2.5.6.3.1.2. Requirement**.** The ESB solution must provide for accessing data services through loose coupling -- distributed system components which do not communicated directly with each other using “point-to-point” interfaces. This "tier” in the AFRC Data Strategy must allow distributed components to connect indirectly and asynchronously. It must provide the capability for protocol and data transformation and act as a mediation service broker providing rule objects for mediation, routing, transformation, and policies. The solution must have a service publish and subscribe capability, provide security and authentication, and possess a service repository. The solution must integrate with the AFRC enterprise mash-up service, data warehouse, and all industry standard data source types. As services available for consumption expand, the solution must have the capability to integrate with Universal Description Integration (UDDI) repository to make service discovery possible.

2.5.6.3.1.3. Availability. System must be available 24-hours-a-day/7-days-a-week (24/7) (99.9%)

2.5.6.3.1.4. Required Hardware. Government supplied.

2.5.6.3.1.5. Workload. 3 FTEs are anticipated for implementation and sustainment which includes hardware configuration, software configuration, certification and accreditation, security, and integration with the existing AFRC enterprise environment. During sustainment, 3 FTEs are anticipated for operations, maintenance, configuration management, software and hardware upgrades, backups, and configuration changes.

2.5.6.3.1.5.1. **System Administrator for all Enterprise Architecture Tools servers [SC Robins AFB, GA ONLY] (1 FTE)**.

2.5.6.3.1.5.2. **Enterprise Service Bus/ Service Oriented Cloud Environment (SOCE) ~~SOA~~ Developer– [SC Robins AFB, GA ONLY] (2 FTEs).** ESB Developer is responsible for the overall architecture, design, implementation, documentation, and day-to-day operation of effective system-to-system integration between systems and data warehouses on which they depend.

2.5.6.4. **Data Warehouse.** An AFRC data warehouse and a common reference data store are required to provide rapid, reliable access to key data to support the availability of commonly used data, and perform advanced and predictive analytics that will support critical command decision making.

2.5.6.4.1. Current State: The majority of data within the AFRC environment is stored within MS SQL 2012 databases.

2.5.6.4.2. Requirement**.** The data warehouse solution must provide for data integrity, eliminating null data, errors, formatting discrepancies, and redundant data. The solution must ensure that data is cleansed, transformed to a useable format, catalogued, and made available for use. It must integrate seamlessly with the AFRC Enterprise Service Bus (ESB) using Service Oriented Architecture (SOA) industry standards. The warehouse must be capable of consuming data from AFRC unique, AF, and DoD systems. The data warehouse must have an Extract Translate and Load (ETL) capability to consume data from existing database technologies such as Oracle, SQL, Excel spreadsheets, etc…, and transform and store data in a consistent format. In addition to supporting analytics, the data solution must also contain a common reference data store which will contain data frequently used by several/many consumers with the AFRC Enterprise. Solution must integrate with the existing AFRC enterprise backup solution, CommVault.

2.5.6.4.3. Availability. System must be available 24/7 (99.9%).

2.5.6.4.4. Required Hardware. Government supplied.

2.5.6.4.5. Workload. 2 FTEs are anticipated for implementation and sustainment which includes hardware configuration, software configuration, certification and accreditation, security, implementation of data cleansing strategy, training, software and hardware upgrades, backups, configuration changes and integration with the existing AFRC enterprise environment.

2.5.6.4.5.1. **Data Warehouse Database Base Analyst [SC Robins AFB, GA ONLY] (1 FTE)**. Tasks include:

- Installation and configuration of software.
- Physical database design to include denormalizing the models based on potential queries, reporting, and system feeds that will be generated from the tables.
- Database maintenance; maintain the tables as necessary for optimization.
- Backup and recovery; Extensive testing of the backup and recovery processes ability to recover databases within the service level agreement, ability to articulate any data loss encountered, Perform frequent backups – full and incremental as needed.
- Data Replication; Ensures accurate and complete replication of applicable data.
- Security administration.
- Database loading.
- Performance Monitoring and Summary table creation.
- Ad-hoc data manipulation.

2.5.6.4.5.2. **ETL Specialist [SC Robins AFB, GA ONLY] (1 FTE)**. Tasks include:

- The Data Warehouse Application Programmer (ETL Specialist) is responsible for applying transformation rules as necessary to keep the data clean and consistent and therefore usable by the user community.
- Programs the data acquisition tool with the rules to be applied to the data.
- Ensures the correct application of the business rules through data query after the data is loaded into the Data Warehouse.
- Applies the business transformation rules.
- Sources the data from the operational systems.
- Prepares a database-loadable file for the Data Warehouse.
- Management of the deployment of the data acquisition tool(s).
- Contributes the technical metadata to the metadata repository.

2.5.6.5. **Mashup Service.** An AFRC Mash-up Service is required to quickly combine data and content from multiple disparate sources into an integrated view to support ad hoc metrics, short fuse actions, what-if scenarios, and other similar efforts.

2.5.6 5.1. Current State. We foresee mashup as an enhanced capability to the AFRC Leadership Dashboard. Ultimately the dashboard will require this capability to dynamically create metrics and perform analysis on a variety of information extracted from both the AFRC data warehouse and also from desperate data sources. The current dashboard has been built within our enterprise SharePoint environment with the potential to be replaced with another solution. At least two dashboards have been created within SharePoint. Next steps include conducting an analysis of alternatives for product selection, procuring the approved solution, and implementing the solution to include hardware.

2.5.6.5.2. Requirement**.** The mashup service must enable users to self-integrate data from enterprise data sources while conforming to enterprise standards for security, reliability and governance. It must provide secure access to data and services from disparate locations and systems, have the ability to leverage data assets, and utilize authorization-based sharing of user created mashups and widgets. This service must integrate with the AFRC Enterprise Service Bus (ESB) and all related components. This solution must be Operations Security (OPSEC) compliant, incorporating business rules that prevent the inadvertent aggregation of classified data.

2.5.6.5.3. Availability. System must be available 24/7 (99.9%).

2.5.6.5.4. Required Hardware. Government supplied.

2.5.6.5.5. Workload. Mashup capability will be expected/delivered 6 months after Government acceptance of ESB. Once Mashup development begins, status/development reports will be due to the Government every 35 days until "mashup" is accepted as functional by the Government.

2.5.6.5.6 Deliverables:

In most cases, the government requirements for an end product or services will be requested by work orders and trouble tickets; however, as manager of common-user systems such as the clients and the base network, the contractor shall initiate and respond to trouble tickets.

Trouble tickets shall be prioritized by the Government in compliance with AFNET prioritized metrics. Specific deliverables and schedule shall be based on compliance with AFNET standards.

Services will be requested and controlled by means of the work orders; work orders will delineate specific objectives, deliverables, and constraints. The contractor shall be responsible for delivering all end items specified in the work orders as well as the work control documentation to the Government Site Lead (or alternate).

2.5.6.5.7. Criteria for Acceptance:

- The Government Site Lead has authority to review or inspect deliverables.

- Acceptance of deliverables and satisfactory work shall be based on the timeliness, accuracy, reliability, and criteria stated in work control forms and the terms and conditions of the task order between the COR and the performing contractor.

2.5.6.5.8. Schedule and Delivery Instructions:

- Deliverables and schedules for delivery shall be as agreed upon and documented on the remedy tickets.
- AFRC reserves the right to rank work orders.

SUBTASK 2 – GLOBAL COMMAND CONTROL SYSTEMS (GCCS)

3.0 PROJECT BACKGROUND. The Air Force Reserve Command, Robins AFB, is responsible for the operation, management, administration, and user Help Desk support for the information technology environment at HQ AFRC, and other local and remote sites. This support will be at HQ AFRC, Robins AFB, GA until otherwise authorized.

The Air Force Reserve Command, Robins AFB, is responsible for GCCS operation and SIPRNET core services. Service objectives include: program and project management planning and execution, network and system administration, and tiered user support initiation/tracking/ remediating for the information technology environment at HQ AFRC, and other local and remote AFRC supported sites. This support is centralized at HQ AFRC and supports AFRC host bases, tenant locations, and others organizations supported by AFRC on SIPRNET. This support will be at HQ AFRC, Robins AFB, GA until otherwise authorized.

In regards to GCCS, NPIRNET and SPIRNET services have only minimally consolidated to date and consolidation efforts are not predicted to have much of an impact on GCCS workload over the next 5 years because the overall labor requirements on SIPRNET are growing.

3.1. Task Specific FIP/Networking Environment:

The HQ AFRC secure network environment consists of 42 locations, 200 servers and 5,000 workstations at multiple buildings and sites. At HQ AFRC about 450 workstations and zero clients are networked to share peripherals, communications and facilities infrastructure.

AFRC uses the following list of standard equipment and COTS software, which will be the primary focus of the task. Non-standard software and hardware will be secondary. Additional brands of equipment and software could be procured during this task order period and will also be covered.

The client has a separate contractor to maintain the hardware infrastructure.

3.1.1. Hardware:

Dell
Cisco
EMC
Gateway
Hewlett Packard
IBM

3.1.2. Standard User Application Software:

Microsoft Office
Microsoft Exchange
NFS and Server Message Block (SMB)
Microsoft SQL (including 2012 and future replacements)
Microsoft SCCM
Internet Explorer
SNMP
MIBS
TCP/IP OSI
Windows Server ~~2003/~~2008/ 2008R2/2012 (and replacements)
Firefox/Mozilla

3.1.3. Network Environment. HQ AFRC is spread out in approximately nine (9) buildings at Robins AFB.

3.1.4. Technical Services Required. The Government reserves the option of assigning additional people at the HQ as well as in the field. Place of performance includes GCCS support for the HQ at Robins AFB as well as future GCCS support for field units.

3.2. Expertise:

- Systems Administration.
- Must be capable of installing, maintaining and upgrading all approved Windows operating systems.
- Must be capable of developing Disaster Recovery Plan for all approved Windows operating systems.
- Knowledgeable of NFS and SMB file system.
- Network Management.
- Must be capable of installing, maintaining and upgrading HP overview.
- Must be knowledgeable of SNMP and MIBs.
- Must be capable of customizing traps in HP Open view to support customer requirements.
- Knowledgeable of Transmission Control Protocol/Internet Protocol (TCP/IP) OSI model for using protocol and analyzer tools.
- Capable of performing network bandwidth subscription calculations.
- Support/Expertise.
- Must be able to set up and administer anonymous file transfer protocol (FTP) services & Computer Based Training modules on CD servers.
- Provide information Protection/Assurance assistance in support of AFRC LAN/WAN.
- Knowledge of virtualization technologies including VMWare and Hyper-V.

3.3. **AFRC SIPRNET/GCCS Senior Network Administrator – [SC] (1 FTE)**. The task requires:

- Operations and maintenance of the AFRC SIPRNET and GCCS within the AFRC MCCC.
- Shall have technical skills and operational experience to assist with supporting both AFRC SIPRNET and GCCS operations.
- Be available to travel on short notice for physical installation of SIPRNET circuits on a case-by-case basis. Projected TDY requirement is 5-7 TDY's per year at least 3 to 4 days.
- Knowledge of virtualization technologies including VMWare and Hyper-V.

3.4. **AFRC SIPRNET/GCCS Network Administrator – [SC] (2 FTEs)**. The contractor shall:

- Provides proficiency administration to install, configure, troubleshoot, manage, maintain and support a Windows ~~2003/2008~~ server and Microsoft Exchange in the stated hardware and network environment, and in the integration of Windows with client user standard application software packages.
- Network administration skills are required in:
  - Windows server products.
  - SCCM and SQL.
  - Motorola Network Encryption System.
  - Mykotronx KIV-7 Encryption Products.
  - Cisco IOS, to include but not limited to experience with Cisco routers and switches, and a thorough understanding of TCP/IP.
  - Knowledge of virtualization technologies including VMWare and Hyper-V.
  - The ability to optimize the Windows server performance and detect and resolve software and hardware malfunctions in a network environment is of paramount importance.
  - Experience in network system administration, management, and maintenance involving communications and microcomputer support functions related to Windows implementation.
  - Knowledgeable of HP Openview.
  - Knowledge of SNMP and MIB.

3.5. **AFRC SIPRNET/GCCS Network Administrator – [SC] (1 FTE)**. The contractor shall:

- Proficient in military management AFSC/skills.
- Network administration skills are required in:
  - Windows server products.
  - SCCM and SQL.
  - Motorola Network Encryption System.
  - Mykotronx KIV-7 Encryption Products.
  - Cisco IOS, to include but not limited to experience with Cisco routers and switches, and a thorough understanding of TCP/IP.

    - Knowledge of virtualization technologies including VMWare and Hyper-V.
    - The ability to optimize the Windows server performance and detect and resolve software and hardware malfunctions in a network environment is of paramount importance.
- Equivalent experience level would be certification as Microsoft Certified Systems Engineer (MCSE) Win 2000 and Cisco Certified Network Associate (CCNA)/CCNP.
- Experience in network system administration, management, and maintenance involving communications and microcomputer support functions related to Windows implementation.

3.6. Deliverables:

- Responsible for delivering a work definition proposal in response to work orders for Client acceptance or negotiation.
- Submits a work completion form with all product deliverables and for services as required by the work order.
- Originals of work control forms are for the Client agency.

3.7. Criteria for Acceptance:

- The Contracting Officer or COR, as delegated, has authority to review or inspect deliverables. The COR may reject or require correction of any deficiencies found in deliverables.
- Acceptance of deliverables and satisfactory work shall be based on the timeliness, accuracy, reliability, and criteria stated in work control forms and the terms and conditions of the contract.

3.8. Schedule and Delivery Instructions:

- Deliverables and schedule for delivery shall be as agreed upon and documented in the work control forms.
- The Government reserves the right to rank work orders.

SUBTASK 3 – ADMINISTRATIVE, PROGRAM MANAGEMENT, ACTION OFFICERS, ANALYSTS, AND SUBJECT MATTER EXPERT (SME) SUPPORT

4.0 ADMINISTRATIVE, PROGRAM MANAGEMENT, ANALYSTS, ACTION OFFICERS, AND SUBJECT MATTER EXPERT (SME) SUPPORT. For other administrative support services, objectives include resource planning and management for the development and implementation of organizational concepts, operations concepts, and integration of functional roles and missions. Products shall be in the form of position descriptions, technical reports, organizational structures, summaries, and formal and informal briefings. This support will be at HQ AFRC, Robins AFB, GA until otherwise authorized.

NOTE: In regards to IT administrative support, pending budgetary actions are expected to create a chaotic environment for manpower in the coming years. This task is written to provide manpower sourcing flexibility administrative support needs are expected/projected to grow, BUT Growth/Increase is not guaranteed.

4.1. **Command Electromagnetic Radio Frequency (RF) Spectrum Support [A6X] (1 FTE)**. HQ AFRC Director of Communications Mission Systems Branch (HQ AFRC/A6OC) has a requirement for electromagnetic RF spectrum support for a wide variety of analytical planning and administrative tasks

4.1.1. These tasks include:

- Implements rules, regulation and policies as established by the National Telecommunications and Information Administration (NTIA), International Telecommunication Union (ITU), Military Communications Electronic Board (MCEB), Joint Spectrum Center and Military Departments to support AFRC operations world-wide. Provide recommendations for guidance on issues relating to and impacting availability of the radio frequency spectrum.
- Engineers, nominates, and assigns frequencies to support Air Force Reserve Command communications, operations and exercise requirements. Reviews and makes recommendations to validate~~s~~ requirements submitted from Command, bases and tenant units, including Land Mobile Radio (LMR) and wireless management duties. Analyzes radio frequency requirements for compatibility with other users of the Electromagnetic spectrum and coordinates frequency needs with federal [Federal Aviation Administration FAA)], military (DoD Area Frequency Coordinator), and civil spectrum agencies [Federal Communications Commission (FCC)] to resolves radio frequency interference and protect national spectrum resources.
- Evaluates new or significantly modified RF equipment detailed in spectrum certification and submit application for frequency allocation and Standard Frequency Action Format (SFAF) in a timely manner throughout the command, and monitors requirements for timely responses from national-level agencies involved in spectrum management. Ensure frequency assignment records in the Government Master File (GMF) and Frequency Resource Record System (FRRS) are up-to-date and maintained IAW governing directives.

- Keeps customers informed of current status on frequency proposals and provide notification of assignment parameters and limitations. Assist organizations from degrading friendly systems or operations during command, control, and communications countermeasures training activities. Make recommendations to AFRC at conferences and meeting with other MAJCOMs, USAF and other military and federal agencies.

4.1.2. <u>Mandatory Qualifications/Expertise</u>.~~:~~ The following the mandatory requirements of this job:

- Must be a graduate of the Inter-service RF Spectrum Management School and the Joint Spectrum Center Spectrum XXI course.
- Experience shall include a range of assignments in technical tasks directly related to the proposed area of responsibility.
- Must be proficient working with Spectrum Certification Software, (SCS) or the Equipment Location-Certification Information Database (EL-CID) Analysis tools.
- Must be knowledge a wide range of communications (radio, radar, concepts, principles), and practices to accomplish work processes through the management of the electromagnetic spectrum.
- Must be able to communicate and explain technical and/or complex information to customers and higher headquarters.

4.2. **<u>IT Requirements Support – [A6X] (1 FTE)</u>**. The HQ AFRC Director of Communications CIO Support Branch (HQ AFRC/A6XC) has a requirement for contractor support to participate in the execution of AFRC CIO functions. The Information Technology Requirements Support position will interact with the Chief of the AFRC CIO Support Branch, the AFR CIO Support staff, other A6 personnel, customers throughout all AFRC functional areas, and AF counterparts. The IT Requirements Support position is anticipated to work independently, interfacing with customers on a daily basis, tracking issues, documenting actions, and providing updates to Government management with minimal oversight.

4.2.1. <u>Requirements</u>:

- Supports the AFRC IT Requirements Program Manager in guiding IT requirements through the AFR IT requirements process, following established AFRC procedures.
- Serves as an A6 customer interface for software development-related requirements.
- Leads the evaluation and processing of requirements related to software development, to include developing potential courses of action for requirements resolution that adhere to AFRC architecture guidance and AF IT compliance issues.
- Works with potential requirements submitters to craft language for submission to the IT requirements process.
- Coordinates with other key players for review of software development requirements.
- Instructs customers regarding AF IT compliance restrictions related to specific software development requirements.
- Tracks software development requirements through the requirements process.
- Assists in the implementation of SDDP within AFR for IT requirements.

- Analyzes new software development-related requirements to determine SDDP and SDDP tiers (per AFRC-defined SDDP Tier delineations).
- Responsible for ensuring requirements owners provide necessary documentation to satisfy SDDP Step 1 (to include the Performance Reference Model identifying end user need(s), relevant LRPs, DOTMLPF-P, stakeholder list, and performance measures).
- Serves as customer interface to assist requirements owners and other key players in navigating completion of other SDDP steps.
- Provides requirements updates, including advocacy of business needs and associated technical solutions to support the AFR IT governance structure (to include CIO Working Group, CIO Board, ECCB, and architectural oversight groups).
- Supports the ECCB process, to include, but not limited to, meeting scheduling, briefing slides, and minutes.
- Supports the AFRC MAJCOM Section 508 program.

4.2.2. Mandatory Qualifications/Expertise:

- Knowledge of common MS Office tools.
- Strong oral and written communication skills.
- Ability to apply knowledge of general SDDP concepts and steps to AFR requirements process.
- Knowledge of AF IT compliance areas.
- Knowledge of AF section 508 expectations.
- Awareness of AF systems and IT technologies/tools and ability to apply these to meet customer mission needs.
- Ability to work independently with minimal oversight.
- Ability to work with a variety of others as either team lead or team member.

4.2.3. Deliverables:

- Tracking mechanism to maintain up-to-date information on the tasks/issues assigned to IT Requirements Support position.
- Weekly status updates to CIO Support Branch Chief, to include new requirements assigned since last update.
- Monthly updates to ECCB (in requested format).
- Proposed ITC effectiveness metrics.
- Time-to-resolution metric.
- ECCB slides and minutes.
- PRM (or AFRC-accepted equivalent) for all for assigned software requirements.
- Meet assigned suspense's for requirements processing (to include requesting extensions, when justified, prior to suspense dates.)
- Recommended solution COAs for each assigned requirement.

4.3. **Voice Switching System (VSS) and Voice Over Internet Protocol (VOIP) Subject Matter Expert (SME) – [A6X] (1 FTE)**. The VSS SME shall assist the MAJCOM Program Manager in reviewing VSS and VOIP requirements, solutions, statements of works, proposals, etc., for technical accuracy and planning of current and future VSS and VOIP implementations at HQ AFRC bases and units. In addition, the contractor will also perform the following duties:

- Provides consulting and engineering services to AFRC for the engineering and installation of all Voiced Switching Systems (VSS) related requirements and programs.
- Determines technical and architectural sufficiency of solutions for VSS requirements.
- Provides independent solution support, independent cost estimates, and evaluate proposed solutions for AFRC VSS and VOIP systems.
- Performs site surveys throughout AFRC, traffic engineering studies, data communications and telecommunications engineering and analysis, architectural studies and analysis and recommend technology insertion initiatives for AFRC VSS equipment.
- Makes recommendations to the Government on activities from an engineering aspect to ensure the latest cost-effective technological solutions are proposed to address customer needs.
- Responsible for technical accuracy, configuration, and pricing of engineering solutions for all VSS and VOIP solutions generated and proposed to the MAJCOM Program/Project Managers.
- Prepares engineering, configuration, and pricing proposals in response to AFRC VSS and VOIP customers' and program/project managers' requirements.
- Provides VSS and VOIP technical support for AFRC Program/Projects Managers to support the implementation of VSS and VOIP requirements and projects at all AFRC bases and tenant unit.
- Provides pre- and post-sales engineering, operations, and technical support for VSS and VOIP equipment purchased to support the AFRC requirements.
- Responsible for reviewing and validating all VSS and VOIP product pricing. Front line experience with VOIP and VoATM services including NORTEL CAIN.
- Develops complex systems engineering proposals and responses to Requests for Proposal/Requests for Quotation for AFRC VSS and VOIP requirements, to include Transport Node (SONET), Access Node, Meridian Mail, Magellan and Meridian Passport, and Meridian 1 product.
- Develops detailed engineering and installation specifications and drawings for Nortel/Avaya/Cisco equipment.
- Provides presentations and briefings concerning status and condition of AFRC VSS and VOIP equipment.
- Provides consulting, training, installation, program management, technical support and engineering services to AFRC for the support of both the VOIP and Telecommunications Management System (TMS) programs.
- Determines technical and architectural sufficiency of solutions for VOIP and TMS requirements.
- Makes recommendations to the MAJCOM in the design and implementation of the Voice Protection System (VPS), VOIP, and TMS systems.
- Supports commercial and Government activities from an engineering aspect to ensure the latest cost-effective technological solutions are proposed to address customer needs.
- Performs site surveys at Robins AFB and associated AFRC bases, traffic engineering studies, data communications and telecommunications engineering and analysis,

converged networks technical analysis, architectural studies and analysis and recommend technology insertion initiatives as they relate to VOIP and network systems.

- Travel will be required to provide consulting, training, installation, program management, technical support and engineering services to AFRC and its associated bases for the support of the VSS, VOIP networks and TMS Programs.

4.3.1. Mandatory Qualifications/Expertise:

- Possess 5 years' experience overseeing the various telephone switches in the AFRC inventory to include, Nortel MSL-100, Nortel Meridian 1, Nortel CS-1000, Avaya/Lucent G3/8700, telecommunications switching equipment, Category 5 through 6 building distribution systems, fiber optic cable distribution systems and copper distribution systems.
- Have at least 2 years' experience with both inside/outside plant telephone distribution system.
- Possess experience with Cisco Call Manager and Unity Messaging Systems.
- Possess experience with Cisco network switches and configurations.
- Proficient in configuration of Nortel/Avaya/Cisco products to support lines, trunks, SS7, CLASS, Meridian Mail, ACD, ISDN Basic Rate Interface (BRI) and Primary Rate Interface (PRI), and associated products including SONET transport systems.
- Specific experience with the interface of TMS and VPS equipment to various telephone switches in the command's inventory to include, Nortel MSL-100, Nortel Meridian 1 and Nortel CS-1000, Avaya/Lucent G3/8700 as well as other telecommunications switching equipment.

4.3.2. Deliverables. The Contractor shall provide:

- Site survey reports, as required.
- VOIP installation and reliability metrics, as required.
- Program updates, as required.

4.4. **Resource Planning and Management [A6X] (1 FTE)**. The contractor shall provide to HQ AFRC/A6 resources planning and management for the development and implementation of organizational concepts, operations concepts, and integration of functional roles and missions. Products shall be in the form of position descriptions, technical reports, organizational structures, summaries, and formal and informal briefings.

4.4.1. Projects:

- Assists the Government with program management of Generation-II (GEN-II) wireless systems for the AFRC Enterprise.
- Reviews and coordinates of all Command Control Communications Computers Integrated Support Plans (C4ISPs) for A6X.
- Over time, projects assigned to this position will change. New projects will be assigned as older projects go to sustainment or end of life.
- Assists on dashboard projects.

4.5. **MAJCOM ICM Program Support [A6X] (1 FTE)**. As the central point for the Internal Control Measures (ICM) Program, the contractor shall perform the following tasks:

- Upon project approval, coordinates with various functional areas within AFRC to ensure implementation of each separate dashboard project.
- Coordinates with A6 staff, customers, programmers, and contractors to ensure proper ICM implementation.
- Tracks status of Certification and Accreditation (C&A), if required, prior to ICM support implementation.
- Ensures funding is addressed and advocated for by the customer.
- Ensures projects are completed on time.
- Responsible for oversight of any Personally Identifiable Information (PII) issues and proper protection of ICM data.
- Must also work to support life-cycle system support requirements.
- Manages projects to support the planning, scheduling and implementation of programs/ projects throughout their life-cycle within the command.
- Develops documentation (project plans, implementation plans, etc.,); maintaining program/project folders for all assigned projects; through use of the AFRC Information Resource Catalog, which is an on-line web accessible database.
- Coordinates with both the AFRC functional Office of Primary Responsibility (OPRs) and/or Air Force program/project managers to successfully implement projects.
- TDY may be required to attend program and/or project meetings; to meet with AFRC base planners to work implementation and/or support issues with affected AFRC locations. Projected TDY requirement is 4-6 per year.

4.5.1. Mandatory Qualifications/Expertise**:**

- Knowledge of MS Project is required to ensure proper program oversight.
- Be familiar with project management tools (such as MS Project), and use these tools in order to track project status and manage project requirements.

4.5.2. Deliverables:

- The contractor shall provide ICM status reports, as required.
- The contractor shall provide and present ICM program updates, as required.

4.6. **Video Teleconferencing (VTC) Subject Matter Expert (SME) and VTC Program Support [A6X] (1 FTE)**. This position will serve as VTC SME for AFRC. As such, the contractor shall perform the following tasks:

- Manages 60 classified and unclassified VTC sites throughout the Continental United States (CONUS).
- Serves as Primary POC for the VTC equipment at 10 VTC suites within HQ AFRC at Robins AFB, and two VTC Hubs (one each unclassified and classified).

- Handles all C&A issues related to these systems.
- Prepares all supporting artifacts for all C&A efforts, and serves as lead in handling our technical refresh (recapitalization program).
- Serves as the AFRC POC for all VTC matters with DISA and the AF Designated Approval Authority (DAA).
- Assists the COR as the command POC for any new VTC systems and/or upgrade to secure video teleconferencing.
- Interfaces with contractors for all maintenance support issues, creates and tracks trouble tickets for all maintenance actions.
- Provides level-1 trouble shooting for VTC and A/V systems and oversees the installation/modification of new VTC equipment.
- Manages VTC equipment for the AFRC VTC hub, and is responsible for working crypto (TACLANE and KIV-7M) support requirements.
- Assists customers in ordering and configuring TACLANE and KIV-7M encryption devices for their sites, as required.
- Coordinates training for HQ AFRC VTC personnel on the AFRC VTC hubs and end user VTC hardware.
- As the VTC SME, makes program recommendations to the AFRC staff and contractors to include the transition from ISDN to VTC over IP.

4.6.1. Deliverables:

- The contractor shall provide VTC usage metrics on a quarterly basis or, as required.
- The contractor shall provide VTC program updates, as required.

4.7. **Enterprise Architecture (EA) Program Analysts [A6X] (6~~5~~ FTEs)**. The contractor shall provide Enterprise Architecture (EA) support services to enhance and manage Air Force Reserve Command (AFRC) EA capabilities. This requirement includes the solutions that integrate existing and evolving governance, EA tools, frameworks, methodologies, models, and artifacts. The solution shall support standard modeling notations as set forth in the Organizational Transformation Framework for Assessing and Improving EA Management, modeling tools (import/export from models) and the storage of artifacts and work products in a single place with version control and configuration management. It shall also provide executives, managers, staff, and authorized contractors a place to design, capture, view, and collaborate on the information that defines how AFRC operates within the one military operational EA net-centric arena.

Services and Support for the EA effort encompass/delivery of five Department of Defense (DoD) Government Accountability Office (GAO) models to include Business, Performance, Data and Information, Service Component and Technical Reference models.

Contractor shall develop and utilize architecture to unravel the complexity of the Air Reserve processes, data, and applications to reveal interdependent relationships, in an easily understandable format, for decision-makers. EA is used as a tool to eliminate redundancy, build efficiency, and optimize utilization of resources. The AFRC EA program will: utilize the DoD Architecture Framework (DoDAF); consider the current ("as-is") and target ("to-be") architecture; and develop transition plans for migrating from the current to the target architecture. Specific guidance for developing AFRC products can be found in the AFRC EA modeling standards governance document. The AFRC architectural segments will be created by utilizing each of the existing AF domain EA and adding AFRC unique business architectures, data architectures, and application architectures.

Contractor shall develop and utilize the Service Development and Delivery Process (SDDP) as prescribed in AFRC SDDP Guidebook in order to improve the definition, design, acquisition, implementation, and delivery of warfighter capabilities. In doing so, the contractor shall provide strategic analyses to assist in the evolution of the AFRC EA program. The contractor shall provide expertise in the development of the EA roadmaps, capabilities-based architecture (compromised of views, methods, data, and relationships). The contractor shall develop EA artifacts in accordance with AFRC, Air Force, and DoD guidelines.

4.7.1. **Scope**. The scope of EA services and support will be associated with all business investments made by and on behalf of the AFRC organization. These services include governance support, design and review, EA technical support, and inter / intra-department collaboration services. These services and support provide technical assistance, technical assessment assistance, and technical expert assistance in support of Strategic planning for Enterprise information Management & Technology, Enterprise Information Architecture Development & Implementation, Capital Planning & Investment Management, Enterprise Management, Strategic Data Sourcing, Collaboration & Knowledge Management and Technology Strategy.

EA Services and Support will address IT system integration and business processes that improve business practices by analysis of the process, and applying information technology components through the DoDAF. System integration encompasses all activities necessary to develop and deploy an information system. It includes the integration of technical components, organizational components and documentation. The information technology components are engineered and integrated into the business process functions. The area of system integration and business process may make use of program management, technical laboratories, prototypes, pilot systems, and tools/methodologies germane to business analysis and business processing reengineering. A non-exhaustive list of examples of the type of work to be performed under this task area is:

- Gap Analysis (“As-Is”, To-Be”).
- Benchmarking EA Integration Activities.
- Business Process Reengineering.
- Test and Evaluation Services.
- IT Solution Analysis.
- Financial Analysis (Make/Buy Decisions).
- Return on Investments (ROI).
- Feasibility Studies.
- Market / Trade Studies.
- System Design Alternative (SDA) Studies.
- Archival Analyses.

The contractor shall develop AFRC EA strategies, transition plans, IT gap analysis, and artifacts for the AFRC EA program. The contractor shall provide support that ensures the AFRC EA is federated to the AF EA. The contractor shall perform analyses in the AF and AFRC component EA spaces as well as the EA sub-domains, i.e., business, data, applications, technology, with emphasis on aligning business strategy and EA with data management/data governance. The contractor shall place special emphasis on the analysis and document business functions and EA system requirements for the AFRC agencies while leveraging Joint DoD Operational/Business Architectures.

4.7.2. **Description of Services**. The contractor shall develop DoDAF artifacts for submission to the Business EA (BEA)/Architecture Compliance and Requirements Traceability (ACART^{TM}) tool as defined in the DoD BEA. The contractor shall format the architectural artifacts to be generated in IBM Rational System Architect. The AFRC stakeholders will review the DODAF artifacts to ensure compliance. The latest version of DoDAF and BEA standards are to be implemented upon official release of use. The AFRC/CEA is the AFRC approval authority for all AFRC EA artifacts.

The contractor shall support the AFRC Chief EA office, i.e., AFRC/CEA efforts. The contractor shall ensure AFRC EA strategies and artifacts are integrated across AFRC functional domains so that the AFRC EA provides a holistic view. The contractor shall assist the AFRC CEA office integration efforts for all EA-related planning, management, investment, evaluation, and revalidation efforts to meet AFRC's operational and business objectives.

4.7.3. **EA Governance Support**:

The contractor shall provide design analysis and recommendations on all investments that impact AFRC operations. Support to the Government includes:

- Conduct analyses of business and/or technical alternatives to support portfolio management regarding system convergence and investment optimization.
- Promote least restrictive acquisition and engineering approaches such as service architectures.
- Conduct EA requirements analysis to identify capability gaps and align investments to strategies.
- Conduct design analyses and assessments to support legacy environment re-engineering.
- Define target architectures for legacy environment re-engineering.
- Develop plans and strategies to re-engineer legacy environments to the target EA.
- Assure AFRC compliance with USAF processes and procedures; evaluate DoD and USAF architectures, directives, instructions, and guidance to assure compliance. Identify DoD and USAF strategies, guidance, and policies and validate applicability to AFRC.

4.7.4. **EA Technical Writing and Documentation**:

The contractor shall be accountable for producing technical documents that describes AFRC EA. These documents will support consultative, informative, and communicative purposes. The contractor shall work with all stakeholders and EA team members to design and develop the processes and artifacts to enable the effective communication of our EA.

- Develop templates to support appropriate document generation standards and manage the versions.
- Generate interactive (html) version and other MS-Office managed versions.
- Design and develop communication products to accommodate EA requirements processes.
- Review the effectiveness of AFRC's EA technical documentation and communication products.
- Complete documents according to our published guides for style, clarity, accuracy, conciseness and terminology.
- Work with developers and other writers to establish technical specifications and to determine subject material to be published.
- Review published material and recommend revisions or changes in scope, format and content.
- Create or modify drawings, illustrations, charts and diagrams to illustrate written material.
- Review competitive products and documentation to further improve our documentation and processes.
- Ensure documentation meets standards and quality control guidelines.
- Develop and maintain installation manuals, administration and configuration documents, how-to guides, release notes and online help files for both customers and employees.
- Serve as the EA program Scribe to record the meetings participants' comments so that the group can see and reflect on the key points under discussion. The Scribe functions as the right hand of the meeting facilitators, freeing them to concentrate on maintaining the focus and flow of the conversation while the scribe writes.
- Develop/maintain EA performance metric statistics and briefings, as required, by AFRC EA Program Management process.

4.7.5. **EA Design and Review**:

The contractor shall create and provide quality assurance on design artifacts and related documents IAW latest version of DoDAF and subsequent revisions, DoD standards, AFRC EA standards (such as the AFRC EA Committee Architecture Framework), AFRC EA Standards, and policies.

- Conduct engineering analyses, modeling and assessments of architectures.
- Promote/develop service architectures to replace legacy environments and implements new capabilities.
- Document 'As-Is' architectures to address capability gaps for the purpose of incorporating enterprise technical, business and data standards into the architecture to meet the National Defense Authorization Act (NDAA) requirements.
- Design target (To-Be) architectures to address capability gaps.
- Evaluate and recommend emerging and evolving technologies and solutions.
- Reengineer enterprise business processes.
- Review and document architectures for architectural design quality and standards compliance.
- Develop and maintain Architectural artifacts required by the USAF EA that represent the unique mission, capabilities, and systems at AFRC.

- Deliver appropriate updates to the EA Governance to identify architecture alignment criteria for approval and certification.
- Deliver AFRC Segment(s) of the USAF EA with goal of federating AFRC architecture with the AF EA.
- Develop transition plans for system convergence and architecture integration.
- Perform Analysis of Alternatives in the form of Initial Market Surveys (Also called Preliminary Analysis of Alternatives).
- Develop and promote Change Management analysis studies in conjunction with the AFRC A6 Workflows Division.
- Develop requisite EA views of mission capabilities and processes along with how those processes are supported through information provided or developed by AFRC and subscribed to and/or utilized by AFRC.
- Utilize the Federal Segment Architecture Methodology to develop AFRC segment architectures. Provides proposed approach and recommended level of detail of each segment.
- Define, subject to AFRC EA Team approval, the requisite set of EA artifacts and the fidelity of those artifacts to expand the EA architectural views. Artifacts may vary depending upon scope of selected architectural projects. Artifacts must be delivered using the AFRC EA repository tool, System Architect (SA). Other software products may be used, as needed, when SA does not contain the necessary features. Artifacts shall be developed in accordance with DoDAF and shall comply with established AFRC architecture standards.
- Develop, maintain, and utilize the Service Development and Delivery Process (SDDP) to analyze and support new requirements. Assist/facilitate requirement owners with delivery of SDDP Step 1 and 2 products to include Performance Reference Models (PRM) and Business Reference Models (BRM). Generate Step 3 products to include Service Reference Models (SRM), Data Reference Model (DRM), Technical Reference Model (TRM), and bounded user requirements. Bounded user requirements must be of sufficient detail and clarity to be executable by both in-house and outsourced material solution providers.
- Transformation Alignment -- Assist Directorates with cultural-shift to Enterprise/net centric-solutions and IT governance discipline.

4.7.6. **EA Technical Support.** The contractor shall provide analysis recommendations and maintenance of EA tools, Sand-box environments, and processes to develop and maintain tools and methodologies which support EA design activities, develop and maintain EA standards and processes (e.g. Standard Architecture templates used in architectural design), provide artifact access to qualified AFRC stakeholders and partners, and develop tools and methodologies to support service lifecycle management activities. Technical support also includes Backup/Recovery procedures and activities for all EA tools implemented.

4.7.7. **EA Intra / Inter-Department Collaboration Service**:

Enhances collaboration with executives, managers, staff, authorized contractors, and any other AFRC stakeholder, within, and external to AFRC (stakeholders and partners), who impact the design of AFRC enterprise.

- Conducts enterprise-wide and cross-domain engineering and architectural analyses and review.
- Provides training on EA services, processes, tools and methodologies to stakeholders and partners.
- Assists stakeholders and partners in executing their responsibilities while collaborating with the EA team.
- Assists AFRC with the development of Analysis of Alternative studies in a preliminary standardized format (A template will be provided by the Government).
- Coordinates participation of AFRC in applicable AF Communities of Interest (COIs). Makes recommendations for participation in applicable AF COIs. Recommendations should include AFRC applicability and interest along with high-level objectives associated with participation in the particular COI. Identify AFRC requirements and align with AF COIs.

4.7.8. **AFRC Unique Application Gap Analysis/Transition Plans.** The contractor shall prepare transition plans for migrating AFRC unique applications to Total Force applications or the Service Oriented Cloud Environment by conducting Fit Gap analysis. The AFRC long term strategy is to utilize DoD and/or AF systems as target applications to the maximum extent possible. The Fit Gap analysis will include the complete Fits with the Total Force target system, the partial fits, as well as the Gaps. The Fit Gap analysis shall depict the AFRC unique needs that are not included in the Total Force System. The proposed plans should include maximizing reuse, reducing duplication, and increasing efficiency. The contractor shall place special emphasis on the Human Capital Management (HCM) and the Financial Management domain. The AFRC unique applications will be prioritized by the government. The contractor shall submit the plans in accordance with the PWS for government review and approval.

4.7.9**. Deliverables.** Specific tasks are as follows:

4.7.9.1. EA Annual Operating Plan:

The contractor shall develop a roadmap for implementing the Air Force Reserve Command's EA program. The EA Annual Operating Plan will be updated on an annual basis (September time frame) and completed within 60 calendar days. Furthermore, it will be maintained throughout the life of the task order with status updates provided quarterly by the contractor to AFRC leadership and key stakeholders. The program management plan shall be approved by the Government. This plan is an operational plan containing of essential program/project planning summary information for use by executive management.

The EA Annual Operating Plan shall be used to manage, track and evaluate the Contractor's performance, specific project progress, and overall program health. The EA Annual Operating Plan shall consist of control policies and procedures IAW standard industry practices for project administration, execution, and tracking. The AE Annual Operating Plan components shall include, but not limited to, the following:

- An Integrated Master Management Plan (IMMP) describing the Contractor's overall management approaches, policies, and procedures including suggested project metrics.
- Identification of Enterprise Architecture milestones or phases where Government information/activity is required and proposed timeline dependencies, if any, for subsequent Contractor activities.
- A detailed staffing plan (hierarchy/matrix) and work breakdown structure (WBS).
- EA sub-project status/progress.
- Identification and projected actions and resolution timelines issues.
- Accounting for resources and reporting.
- Conclude with analysis and recommendations.
- It may include such areas as life-cycle management reviews, impact assessments, as well as providing administrative and management planning support for analyzing, developing and updating policy and planning documents.

4.7.9.2. **AFRC EA Operational Support.** The following items identify and outline EA operational support objectives, staging, implementation and management of AFRC EA work and tasks. The deliverable is a collection of documents and activities. The contractor shall:

- Generate and/or maintain enterprise business, information, and technology architecture standards guidance, governance plans, and analysis reports.
- Produce and/or collaborate with other entities to create EA graphical views ("artifacts") for existing or new systems or applications, utilizing the latest versions of IBM Rational System Architect software tool and XT add-ons, in accordance with published architecture compliance guidance such as the AFRC EA Committee Architectural Framework, DoDAF standards and AFRC Architectural Standards.
- Collaborate horizontally and vertically across multiple organizations as well as manage projects to support AFRC CIO and IM/IT transformation initiatives.
- Utilize the latest tools, industry knowledge, and expertise to implement and promote EA compliance across the AFRC as directed by DoD, USAF and AFRC.
- Create and deliver guidance and status briefings to Air Force leadership.
- Maintain a strategic "as is" and "to be" AFRC OV-5 and AV-1 and collaborate with the intra/extra Joint operational/business activity models (OV-5), as needed, and evaluate and make recommendations for incorporation of Joint operational/business architectures.
- Develop, or update and maintain an AFRC EA governance process diagram and an AFRC EA Board Charter.
- Develop and maintain agendas, minutes and EA metric slides for EA Board meetings.
- Work with the AFRC Government Chief EA or designated representative to devise and document an AFRC "to be" business, information and technology EA strategy/vision.
- Draft and/or maintain/revise/edit and distribute AFRC CIO EA Compliance Guidance and EA Evaluation Checklist.
- Analyze the existing "as-is" business, information, technology architectures of AF and Joint operational/business applications architectures and provide written recommended steps needed to transition to "to be" state when required.
- Develop a strategy for linking/de-duplicating and tracing solutions architecture artifacts with other DoD, USAF and AFRC HQ agencies.

- Develop a slideshow to market EA internally to the AFRC organization.

4.7.9.3. **Initial Market Surveys (IMS) / Preliminary AoAs (PAoA).** A compliant IM/IT investment review for new or existing systems requires a thorough Initial Market Survey or Preliminary Analysis of Alternatives (PAoA). As new or existing requirements traverse the acquisition or modernization process, the contractor shall:

- Prepare and produce IMS/PAoA reports to include summary, background, explanation of alternatives and a formal prioritization, an alternative selection recommendation, along with justification for selection.
- Apply an evaluation methodology and format (approved by the government) for AFRC Initial Market Surveys Preliminary AoA/IMS studies and reports. There may be instances where multiple PAoA/IMS's are required to be completed concurrently although this is expected to be rare.
- Study in-depth requirements and functional capabilities for proposed or existing systems, applications, modernizations, upgrades, or transition staging projects
- Research requirements, compare/contrasts needs and capabilities to existing Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) products, and/or developed solutions.
- Produce reports within a reasonable period of time based on the complexity of the requirements analysis, on average 2 to 4 weeks.

4.7.9.4. **Business Process Re-engineering (BPR).** The 2010 National Defense Authorization Act requires the addition of a business process re-engineering assertion as part of the Defense Business Transformation (DBT) certification. This means that before a defense "business" system is purchased or developed, that the buyer or agency must first sign a statement that asserts they have accomplished business process re-engineering efforts to first improve the processes' efficiency, ideally leading to improvements and efficiencies of any automation initiatives. To accomplish this, business processes, and in the case of AFRC integrated processes must be dissected, diagrammed, and analyzed for inefficiencies, then reassembled and re-diagrammed to eliminate identified inefficiencies. The newly "re-engineered" processes become part of the IM/IT project or design. As new or existing requirements traverse the acquisition or modernization process, the contractor shall:

- Identify all Business Process Reengineering (BPR) and operational workflow mapping efforts throughout the AFRC and compile a report on the types and maturity of activities and methodologies.
- Research and recommend business process management and BPR tools.
- Identify and gather "as-is," and when available, "to-be" business process reengineering drawings, artifacts, workflow diagrams, process flow charts, and OV-6c diagrams from varying/disparate AFRC systems and applications into a single location/repository with a standard file naming convention.
- Apply a proven business process reengineering methodology, (e.g., AFSO21, LEAN Six Sigma or similar, to analyze and improve processes).

- Attend requirements, subject matter expert, consultant, and high performance team meetings and facilitates process mapping, diagramming, and reengineering to document new "as-is" and "to-be" BPR activities.
- Create BPR reports and Business Process Management Notation (BPMN) diagrams (DoDAF OV6c diagrams) utilizing IBM System Architect or compatible/comparable substitute visualization tool.
- Share and ensure BPR activities are linked into applications/solutions architectures and as well as the BRM, PRM, DRM, SRM and TRM, models in addition to the EA training and skill needs requirements.
- Maintain BPR diagrams in a library or repository and make them available to applications developers and other contracted vendors, as needed.

4.7.9.5. **Decision Support Services.** Architecture products may be used at all organizational levels to help managers and decision makers achieve maximum effectiveness, efficiency, and economies of scale from IM/IT investments. To aid decision makers the contractor shall:

- Collaborate with Portfolio Managers to establish a comprehensive AFRC systems inventory.
- Engage in the requirements and business capabilities lifecycle (BCL) acquisition process and aid in the identification of potential duplicate capabilities or existing re-useable capabilities.
- Create architecture decision support reports showing overlapping or duplicate capabilities, and recommend system/application transition, consolidation, and sun-setting actions.
- Research and obtain alternative points of view (i.e., Joint Interoperability/Operations) to avoid limited judgment on critical EA issues.
- Assist/gather/provide architecture information for Analysis of Alternative reports.
- Obtain advice regarding EA developments in industry, university, or foundation research.
- Enhance the understanding of, and developing alternative solutions to, complex EA issues.
- Update and advise AFRC decision makers on architectural compliance.
- Obtain opinions, special knowledge, or skills of noted EA experts.
- Research and review existing EA standards and develop new EA policies and procedures.

4.7.9.6. **DoD, USAF and AFRC EA Compliance.** To ensure compliance with DoD, USAF and AFRC EA the following specific activities and services will be performed by the contractor. The contractor shall:

- Establish, maintain, and follow AFRC internal architecture governance processes in accordance and conjunction with existing AFRC governance.
- Adopt, modify or change internal governance processes and structures as needed, or when external guidance requires.
- Review capability, acquisition (e.g. Initial Capability Document, Capability Development Documents, Problem statements, Capability Production Documents and Consolidated Acquisition Management Plans), and DBT documents ensuring compliance with DoDAF, AFRC, and AFRC EA policies, directives and guidelines. Provide timely feedback and assist with document updates and/or the generation of new documents when appropriate.

- Document discrepancies, variances or exceptions to compliance with the AFRC and AFRC EA.
- Prepare and/or update DoD Reference Business, Information, and/or Technical Reference Models, as needed.
- Develop and/or document functional requirement and capabilities reviews which are aligned with the AFRC EA, AFRC Strategic Plan and Information Management (IM)/IT Capital Investment Portfolio Plan.
- Develop and maintain architecture products, data, and process models.
- Develop and maintain system architectural and interface products in accordance with IEEE, DoDAF, and information assurance standards which include mandated systems architecture products, to include system and subsystem performance-based descriptions and key interfaces and input data into the AFR System Architecture Repository. System architecture must clearly show requirements traceability to the operational architecture in the AFRC EA.
- Develop and maintain a Technical Standards Profile (StdV-1, StdV-2) using the online DoD Information Systems Repository (DISR) template available at https://acc.dau.mil. Input data or artifacts into the DISR Online System.
- Provide input data and artifacts into the AFRC Systems Inventory Reporting Tools.
- Input data or artifacts into the DoD Architecture Registry System (DARS).
- Collaborate with AFRC A6 CIO, Command CTO, and functional areas to establish and maintain the Data/Information Reference Model and Technical Reference Models.
- Develop or maintain a “Fit for Purpose” architecture compliance requirements checklist
- Perform analysis of new and existing AFRC applications and systems to provide Program Management Offices (PMOs) and application developer’s advice and consultation reports on architecture compliance status and transition action recommendations.

4.7.9.7. **Required Architecture Artifacts.** AFRC/A6 serves as the entry point for new initiatives in the requirements process. In doing so, we also serve as the focal point for the development of EA artifacts after attendance at any Intra/Extra Departmental requirements effort. There are several artifacts that must be developed in order to assure that potential or existing investments have adequate architecture completed. The contractor will produce the following artifacts NLT 120 days following completion of any requirements set-forth and approved by AFRC EA stakeholders. The Artifact list is as follows: AV-1, AV-2, OV-1, OV-2, OV-5a, OV-5b, OV-6a, and OV-6c. This is the minimum acceptable architecture that must be delivered, but is in no way indicated to be a complete list of architectural artifacts that may be required.

4.8. **IT Equipment Control – [SC] (1 FTE)**. Tasks include, but not limited to:

- Schedules classroom and provide training to Equipment Custodians (ECs) at Robins annually.
- Prepares quarterly EC training update to keep EC’s current on procedures.
- Maintains listing of donation eligible customers to receive excess equipment.
- Maintains all accountability for excess equipment through inventory database.
- Prepares documentation for asset, deliveries, secure storage, and transfer functions.

- Utilizes Asset Inventory Management (AIM) to add, edit, and deleting IT asset records to provide management reports.
- Assists with IT inventories and Reports of Survey.
- Provides ECs with current inventory listings.
- Packages may weigh as much as 50 pounds each as part of performing duties above.
- Provides backup support for 4.9.

4.9. **Support Services, Package Delivery and Receipt of IT Equipment – [SC] (1 FTE)**. Tasks include, but not limited to:

- Provides services for receiving, processing, distributing, and dispatching official and accountable mail and administrative communications for HQ AFRC supported activities. These services must be IAW DoDM 4525.8, *Official Mail Manual*, DoDM 4525.6, Vol II, *Military Post Office Operation Procedures*, Domestic Mail Manual (DMM) and the International Mail Manual (IMM). Organizations receiving Support: HQ AFRC, 951st Reserve Support Squadron (951 RSPTS), and RMG.
- Using the existing secure mail distribution room/boxes, stores received express mail/packages of IT equipment.
- Receipts for express mail/packages from private carriers in the HQ AFRC Director of Communications Programming and Execution Branch (HQ AFRC/A6XR) duty section (the basement of Building 210).
- Capable of lifting up to 50 pounds as part of performing duties above.
- Postal/parcel services include receipt, storage, distribution, and accountability of packages containing IT equipment.
- Establishes a self-help express mail center in the basement of Bldg 210 for receipt and delivery of IT equipment.
- Assists customers in preparing express mail for pickup and to accept express mail deliveries of IT equipment.
- Provides backup support for 4.8.

4.10. thru 4.21. RESERVED

4.22. **Cyber Force Readiness [A6 Force Readiness Branch (FRB)] (1 FTE)**. The contractor shall provide analysis support to the Force Readiness Branch within A6.

- Responds to assigned taskers from the Force Readiness Branch (FRB) Chief on issues pertaining to the FRB functions and tasks.
- Develops, defines, and documents new or evolving metrics and demographics for functional managers and other customers within the FRB.
  - Accomplishes 95% changes to existing metrics/demographics within 7 working days.
  - Develops 95% of new metrics/demographics within 14 working days.
- Provides data analysis on metrics and demographics for all FRB functional managers.
- Provides data analysis on billets for MAJCOM Functional Managers (MFMs) for purposes of metrics and tracking changes in end strength.
- Briefs the A6 and/or AFRC leadership on the analysis of various MFM products.

- Reviews, researches, coordinates, and utilizes Unit Manning Documents (UMDs), Unit Manpower Personnel Roster (UMPRs), Unit Training Assembly Participation System (UTAPS), Air Force Reserve Orders Writing System-Reserve (AROWS-R), and other documents for various tasks in creating accurate MFM documents and briefings (e.g., Cyber Health Briefs for all AFSCs: 17DXX, 3DXXX, 1B4XX, 3A1XX; Staff to Staff submittals, all status allocations by MAJCOM/COCOM/Agency).
- Reviews, researches, coordinate and assists in writing position descriptions for Cyber billets.
- Provides SharePoint site administration and Training Business Area (TBA) for the FRB.
- Manages SharePoint site setup, issue and update new SharePoint accounts/permissions, customized workstations, file shares, and posts information for retrieval.
  - Ensures 80% of all tasks are completed within 3 working days.
- Develops and assist MFMs in creating routine functional newsletters to the field.
- Drafts Standard Operating Procedures (SOPs) for tasks accomplished within the FRB and create analysis on related products.
  - Ensures 80% of all tasks are completed within 14 working days.
- Registers, tracks, and monitors attendees for various cyber training courses.
  - Ensure 75% seat fill rate for each class offering in Cyber classes (e.g., Cyber 200/300).
- Provides support for pre/post-Development Team (DT) tasks.
- Performs other tasks duties as required by the Force Readiness Branch.
- Performs submission of metrics entering the Internal Control Measure (ICM) tool process.
- Ensures adherence of standards on submittals to ICM Business Rules.
- Reviews, tracks and collates position data across all statuses (AD, AGR, ART, IMA, and TR): specifically vacancy/fill rates, pending change actions such as reorganizations, IMA Internal Program Reviews (IPRs), Program Objective Memorandum unit activations/deactivations, and other programmatic changes.
- Provides Task Management Tool (TMT) submittal/response data for tasker completion to FRB.
- Develop and assist MFMs in routine position vacancy announcements to the field.
- Provide support for the career field demographics.
- Provides monthly activity report outlining completed/in process tasks to A6OD branch chief.
- Engages FRB and MFMs on records management status, develops standard business rules (such as location, access, and classification of records) and employs said rules where appropriate.

4.22.1. Deliverables:

- Briefings.
- Draft and final standard operating procedures and business rules for the functional managers, as required, are accomplished within 14 working days.
- Position Descriptions both military and civilian.
- Current and projected position data across the cyber position enterprise.
- SharePoint administration/maintenance.

- Document reviews (e.g., UMDs, UMPRs, FUSE, SOPs, briefs, UTAPS, AROWS-R) are accomplished within 14 working days.
- Other documentation or briefings, as required by the FRB.
- Monthly activity report.

4.23. **Master Calendar Functional Administrator [A6XP] (1 FTE)**. The contractor shall provide project management and daily execution update support as the Command central point of contact for the Master Calendar including the following tasks:

- Provides functional project management and administration of the AFRC enterprise-wide Master Calendar process to provide recommendations on process improvement, metrics, and evaluate enhancements for potential inclusion in the Calendar management process.
- Provides recommendations for new calendar content.
- Implements processes to avoid or resolve conflicts of long range planned events.
- Seeks sources of Master Calendar content.
- Coordinates MAJCOM Master Calendar content and maintain status tracking in the Command Master Calendar.
- Validates content and currency of MAJCOM Master Calendar.
- Defines and publishes, with COR approval, MAJCOM Master Calendar business rules and schedule.
- Maintains and updated the AFRC Master Calendar Guide, as required.
- Briefs MAJCOM Master Calendar alternatives, events and to senior leadership, as required.

4.23.1. Mandatory Qualifications/Expertise:

- 5-7 years' experience in MS products, including MS Project and SharePoint 2010
- Experience as a Lead Project Manager
- 3-5 years' experience in enterprise information systems and Knowledge Management
- Possess excellent verbal and written communications skills.

4.23.2. Deliverables:

- Provides updates to the Master Calendar governing documents, as required.
- Provides Master Calendar status reports and metrics, as required**.**

5.0 GENERAL INFORMATION:

5.1. Organizational Conflict of Interest (OCI) Avoidance. To prevent conflicting roles that may bias the contractor's judgment or objectivity, and to preclude the contractor from obtaining an unfair competitive advantage in concurrent or future acquisitions, the contractor will be restricted as set forth below:

The Contractor shall be familiar with the Federal Acquisition Regulation (FAR), Part 9, Subpart 9.5, entitled “Organizational and Consultant Conflicts of Interest,” and agrees to avoid conflicts of interest IAW the principles set forth in this subpart. Since the Contractor under the terms of this task order will have access to Government and third party data which might place the Contractor in an OCI, the Contractor agrees to perform this task order as set forth below:

To refrain from unauthorized use or disclosure to any individual, corporation, or organization of any data. advice, trade secrets, software, confidential financial information, proprietary or restricted information, to include FOR OFFICAL USE ONLY information (collectively referred hereinafter as “data”) of the Government or other companies coming into its possession in connection with the work under this task order for as long as it remains proprietary.

To establish associate contractor relationships by executing written agreements between companies having a proprietary interest in such data. These agreements shall prescribe the scope of authorized use of such data as well as necessary safeguards against unauthorized use or disclosure. A copy of the agreement shall be furnished to the Contracting Officer promptly after execution of the task order.

The contractor shall formally train its employees, in regard to OCI, that they shall not divulge proprietary data obtained from other companies or from the Government to anyone except as authorized in writing. The contractor shall require its employees to execute certificates attesting to their training and understanding of the requirements to safeguard all sensitive information. The contractor shall warrant that its employees shall not use for their benefit any data, advice, trade secrets, confidential financial information, proprietary or restricted information (to include FOR OFFICIAL USE ONLY information) that the employee received in connection with this task order, during or subsequent to the term of his employment.

To obtain from each of its employees, whose responsibility in connection with the work under this task order may be reasonably expected to involve access to such proprietary data or classified information (Government or contractor generated), a written agreement between the company and employee, which in substance shall provide that the employee will not, during employment by the Contractor or thereafter, disclose any such proprietary data or classified information to which the employee had access in connection with the work under this task order.

To refrain from utilizing such data or classified Government information coming into its possession in connection with work under this task order for purposes other than those for which it has been furnished, unless specifically authorized by the organization providing such data or Government information.

To hold the Government harmless for any cost/loss resulting from the unauthorized use or disclosure of third party data or software by the Contractor, its employees, subcontractors, or agents.

The contractor further agrees to insert a provision conforming substantially to the language of this clause, including this paragraph, in any subcontract or consultant/partnering agreement.

The contractor warrants that, to the best of its knowledge and belief, there are no relevant facts or circumstances which could give rise to an OCI, as defined in Federal Acquisition Regulation (FAR) Subpart 9.5, or that the Contractor has disclosed all such relevant information.

If a contractor determines that it, or any potential subcontractor, has an OCI, or a potential OCI, then the contractor shall address the conflict of interest, and shall provide a mitigation plan for the conflict of interest. The mitigation plan shall avoid, mitigate, or neutralize the OCI such that the full scope of work contemplated by the solicitation can be performed by the contractor.

The contractor agrees that if an actual or potential OCI is discovered after award, the contractor shall make full disclosure in writing to the Contracting Officer. This disclosure shall include a description of the actions the contractor has taken, or proposes to take, after consultation with the Contracting Officer, to avoid, mitigate, or neutralize the actual or potential conflict.

The Contracting Officer may terminate this task order for convenience, in whole or in part, if he/she deems termination necessary, to avoid, mitigate, or neutralize an actual or potential conflict. If the contractor was aware of a potential OCI prior to award, or discovered an actual or potential conflict after award but did not disclose it, or misrepresented relevant information to the Contracting Officer, the Government may terminate the task order for default, debar the Contractor from Government contracts, or pursue other remedies as may be permitted by law or this task order.

The general rules in FAR 9.505 prescribe limitations on contracting as the means of avoiding, neutralizing, or mitigating OCI that might otherwise exist in the stated situations. Illustrative examples are also provided in FAR 9.508. The two underlying principles are: preventing the existence of conflicting roles that might bias a contractor's judgment; and preventing unfair competitive advantage by a contractor competing for award.

Except with the prior written consent of the Contracting Officer, the Contractor shall not compete (as a prime Contractor, subcontractor, main supplier, or consultant) during the period of this task order, including any extension thereof, and for one year thereafter, for the award of any task order for, supplies, services, or construction which was generated under this task order. This prohibition does not prohibit the Contractor from competing on the follow-on to this task order.

When a prospective Contractor has an unmitigated OCI conflict or the Contracting Officer (CO) cannot determine fair pricing, the Government reserves the right to exercise some or all of the following rights:

Render Contractor(s) ineligible for award for the specified task order and/or future task order;

Require prospective Contractor(s) withdrawal from at least one team when affiliates participate on two different teams in the same acquisition;

When the Prime Offeror proposes and subcontracts with more than one Prime Contractor for the same effort the Government may evaluate the prospective proposal(s) as high risk that may result in non-award.

The following regulations also apply to this subject:

- FAR 52.203-16, *Preventing Personal Conflicts of Interest* (Dec 2011)
- AFFARS 5352.209-9000, *Organizational Conflict of Interest* (Oct 2010)
- AFFARS 5352.209-9001, *Potential Organizational Conflict of Interest* (Oct 2010)

5.2. **Reimbursable Costs**:

Reimbursable costs must be pre-authorized by the local AO, the COR and GSA contracting officer before performance. Contractor shall submit an estimate in ITSS under an action memo for approval.

The contractor shall ensure that reimbursable costs do not exceed awarded budgets.

5.3. **Travel**. Travel may be required to fulfill the requirements of this task. The contractor shall ensure that the requested travel costs will not exceed what has been authorized in the task order. Contractor incurred actual expenses resulting from Government directed travel are cost reimbursable but are limited by the Government Joint Travel Regulations (JTR) and must be pre-approved by the COR and GSA Project Manager by inputting the request into ITSS through an Action Memo. The contractor shall include any anticipated travel costs in the proposal.

Locations and the duration of travel cannot be established at this time so a not-to-exceed travel budget ~~**of $1,000,000**~~ for the entire effort is estimated. ~~**The base period has a budget estimate of $200,000 and each option year has a budget estimate of $200,000.**~~

Base period Travel Budget Estimate ~~**$200,000.00**~~	**$132,370.32**	~~**$132,842.97**~~
Option Year 1 Travel Budget Estimate ~~**$200,000.00**~~	**$178,886.48**	~~**$178,451.26**~~
Option Year 2 Travel Budget Estimate ~~**$200,000.00**~~	**$174,523.52**	~~**$174,930.70**~~
Option Year 3 Travel Budget Estimate	**$302,823.30**	~~**$200,000.00**~~
Option Year 4 Travel Budget Estimate	**$225,000.00**	
Extension Period Travel Budget Estimate	**$175,000.00**	

5.4. **Training**. Training of contractor employees assigned to this task order shall be performed at the contractor's own expense, with these exceptions:

The Government has given prior approval for training to meet special requirements that are peculiar to the environment and/or operations.

The government client will provide required training that is Air Force specific or unique applications to ensure contractor performance.

The Government will not authorize contractor employees training to attend seminars, symposiums, or other similar conferences unless the GSA Contracting Officer or designee certifies and approves that attendance is mandatory for the performance of the task requirements.

In the event that the Government has approved and paid for contractor employee training, reimbursement shall not be authorized for costs associated with re-training replacement individual(s) should the employee(s) terminate from this task order. Costs that are not authorized include, but are not limited to; labor, travel, and any associated re-training expenses. A not-to-exceed training budget ~~of $225,000~~ for the entire effort is estimated.

Base period Training Budget Estimate	**$48,953.79**	~~**$48,920.72**~~	~~**$30,000.00**~~
Option Year 1 Training Budget Estimate	**$25,423.99**	~~**$25,419.65**~~	~~**$30,000.00**~~
Option Year 2 Training Budget Estimate	**$59,503.63**	~~**$59,096.44**~~	~~**$30,000.00**~~
Option Year 3 Training Budget Estimate	**$15,942.34**	~~**$30,000.00**~~	
Option Year 4 Training Budget Estimate	**$30,000.00**		
Extension Period Training Budget Estimate	**$15,000.00**		

5.5. **Use of Government, GSA Leased, and/or Privately Owned Vehicles (POVs)**. Travel to and from work sites may be required to fulfill the requirements of this task. This provides guidance on what vehicles the contractor can and cannot drive on the Air Force installations in the performance of this task order.

5.5.1. Use of GSA Leased Vehicles:

The Contractor may USE Government leased vehicles to perform any duties in the course of this task order. When contractors or subcontractors of using agencies are in accidents involving GSA IFMS vehicles, the agency employing the contractor will usually be billed directly for all costs associated with the accident. It will be the responsibility of the using agency to collect accident costs from the contractor should the contractor be at fault.

The contractor is permitted to ride as a passenger in GSA-leased vehicles at any time in performance of their obligations under this task order.

5.5.2. Use of Air Force Owned Vehicles:

- The contractor may use vehicles owned by the Air Force, hereafter referred to as “shared use” vehicles, if there is a vehicle currently authorized and/or assigned to the base in performance of this task order.
- Prior to contractor use of a shared use vehicle, the contractor must certify individuals are trained, licensed, and physically qualified to operate the vehicle, and briefed on official use policies. (Reference AFI 24-301, *Vehicle Operations*.)
- If both government and contractor personnel are available to drive said vehicle, then the vehicle will be driven by the government representative.
- Local procedures will be established for the sign-in/out use from the appropriate government representative.

- In the event required work must be accomplished outside the installation, either a government representative will drive the contractor to the work site or the contractor may be required to drive their own POV.

5.5.3. Use of Privately Owned Vehicles (POV):

- The contractor may be required to furnish a company vehicle to perform official duties IAW the requirements of this task order at no cost and no liability to the government. Contractor employees will not be reimbursed for POV/company car expenses used in the local area.
- Request for approval of local travel must be submitted prior to the use of such vehicles via ITSS Action Memo, in writing by the GSA contracting officer or the base communications squadron commander and/or his/her designated representative.
- In the event required work must be accomplished outside the installation, the contractor may be required to drive their own POV to the work site. Mileage may only be reimbursed for direct point to point trips to provide required service.
- Contractor will submit mileage receipts/mileage logs for reimbursement on a monthly basis. Claims will be validated by either the base communications squadron commander and/or his/her designated representative.

5.6. **Performance Criteria**:

5.6.1. Hours of Work:

- Normal duty hours are from 0700-1600 (military); 7:00 AM to 4:00 PM (civilian), Monday through Friday, excluding federal holidays.
- The Government reserves the right to change the core hours at any time.
- Any variation must be negotiated and pre-approved by the Government.
- Flextime is acceptable and reporting time can be between the hours of 7:00-9:00 AM for 8 hours-a-day, Monday - Friday, except government holidays, for each site (not including 30 to 60 minutes for lunch).
- Telework/telecommuting is authorized on an exception basis and only as approved by the COR.
- The Contractor shall support all Unit Training Assemblies (UTAs) or as directed by the COR.

5.6.2. Variance in Regular Hours for Emergency Workload Peaks:

- Occasional emergency workload peaks, or changing government priorities, may necessitate that the Contractor discusses workload priorities with the COR and request the approval of a variance in regularly scheduled hours.
- If the COR cannot rank the jobs in order to meet critical deadlines without affecting predetermined shift composition, the COR may approve a shift variance, if requested.
- This does not constitute an approval for extended hour’s compensation. Rather, the contractor shall realign the scheduling of personnel to preclude the necessity for extended hours compensation.

5.6.3. Extended Hours/Overtime. If extended hours or overtime are unavoidable, hours will be cost reimbursable for this task order on a labor hour basis. If overtime/extended hours are authorized on this task, the contractor must obtain authorization from the COR prior to anyone working overtime. Under no circumstances shall contractor employees exceed the extended hour allotment. If additional extended hours are required, the Client On-Site Lead shall request, in writing, through the COR that the task be amended accordingly.

5.7. **Contractor Recall**. If "after hour's system failure" occurs, the contractor shall provide fully qualified personnel, accessible by phone, on a 24-hours-a-day, 7-days-a-week basis, to perform the unscheduled mission or emergency requirement. For unscheduled mission requirements, contractor personnel shall respond within 30 minutes of the initial notification and be on-site within 1 hour after the initial response in order to perform services and satisfy unscheduled mission requirement. The contractor shall coordinate with the Client On-Site Lead to compensate the contractor (i.e., adjust the contractors work schedule or approve overtime). For planning purposes, all communication units will be authorized to generate "on-call" rosters of GD contractors to be contacted in the event an unscheduled mission or emergency requirement that may occur after duty hours. If a contractor recall is required, the Client On-Site Lead (communications command and/or Senior ART) will either authorize overtime and/or adjust the contractor's work schedule. NOTE: If a contractor recall occurs, and the communications commander/Senior ART authorizes overtime, then he/she will be required to contact the COR within 24 hours of the contractor recall.

5.8. **Telecommuting**. Telecommuting allows written pre-authorization by approving authority to allow contractors to work in an official capacity away from the official duty location. The alternate work locations must have the necessary tools and environment to enable civilians to accomplish assigned duties. All data, documents, or products developed are the sole property of the United States (US) Government and will be prepared for filing IAW command guidance if it is to be a permanent record. Any and all telecommuting agreements/positions will be negotiated after contract award.

5.8.1. Roles and Responsibilities. The COR is the approving authority for all telecommuting and work agreements.

5.8.1.1. Immediate Supervisor. The GDIT On-Site Project Manager is responsible for:

- Recommending the telecommuting project to the approval authority.
- Preparing required documentation and obtaining any necessary signatures from the telecommuter.
- Ensuring project details (e.g., scope of work, deliverables, etc.) are mutually agreed upon before beginning work.
- Quality control of the telecommuter‘s completed product.
- Maintaining the original approved agreement.

5.8.1.2. Contractor. Contractors are responsible for identifying telecommuting equipment requirements to the GDIT On-Site Project Manager.

- Contractor should obtain the approval authority's concurrence before performing telecommuting that exceeds the agreed hours.
- The approval authority of the telecommuting agreement may terminate participation in telecommuting at any time.

5.8.2. Agreement. The contractor and GDIT On-Site Project Manager shall sign an agreement before starting the telecommuting project specifying all terms for the project.

5.8.3. Government Furnished Equipment. Subject to AFI 33-200, *Information Assurance (IA) Management*, AFI 33-112, *Information Technology Hardware Asset Management*, Air Force Systems Security Instruction (AFSSI) 8502, *Computer Security*, and other prescribed rules and limitations, a Commander may approve the installation of government-owned computers, computer software, and telecommunications equipment (hereafter referred to as equipment) in alternative work locations.

- The commander or designated representative retains ownership and control of all hardware, software, and data associated with, or generated by, government-owned systems. The commander must account for equipment on a hand receipt and inventory annually. The commander must notify the Equipment Control Officer (ECO) of the relocation of the equipment (AFI 33-112). Any equipment not returned to the Government shall be paid for by the Contractor.
- Government equipment is FOR OFFICIAL USE ONLY (FOUO). Commanders may authorize installation, repair, and/or maintenance of equipment at their discretion and direction. The equipment is for authorized use by the civilian only.
- The contractor agrees to protect any government-owned equipment from damage, loss, theft and infection with computer viruses.
- Individual contractors are not authorized to install hardware or software on a government system; only unit CSTs have that authority and only with the permission of their unit commander.
- Contractors must follow Report of Survey (ROS) procedures for damaged, lost, or stolen government equipment (AFI 33-112 and AFI 33-114, *Software Management*).
- Government information must be protected from modification, destruction, or inappropriate release.
- Users of Government provided telecommunications in alternative work locations are subject to the monitoring requirements of AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)*.

5.8.4. Equipment Obligations**:**

- Contractors using government owned equipment must sign an agreement outlining the required equipment, software, hardware, data, and telecommunication services.
- Contractors must ensure that software use conforms to all copyright law and any contractual agreements.
- If network connection is required at the alternate duty location, it shall be at the contractor's expense.

- If telecommuting requirements terminate, the contractor must immediately return government owned hardware, software, data, and cancel all telecommunication services that the government provided. (AFI 23-111, *Management of Government Property in Possession of the Air Force* (AFI 33-112, AFMAN 23-110, Volume 2, *USAF Supply Manual*, Part 13, Chapters 4 and 8,).

5.9. **Government Furnished Property**. The government shall provide the facilities (desks , chairs, computers, network access etc…) for up to 9, on base employees.

5.9.1. Government Furnished Facilities. The government will provide a work area for on-site support except for paragraph 5.8. of this PWS.

5.9.2. Government Furnished Equipment. The government shall provide the contract personnel the computer resources necessary to perform these tasks. The contract personnel will have access to Government regulations, specifications, standards, technical manuals, and task documentation during normal duty hours and throughout the duration of this contract. The government will provide office space, to include desks, chairs, tables and telephone support consistent with that provided to the government employees.

5.9.3. Obtaining Replacement of Government-Furnished Equipment. The contractor shall submit requests for replacement of government-furnished equipment to the Quality Assurance Personnel (QAP) for processing. Such requests shall specify the reason for the replacement request.

5.10. **Government-Furnished Services**:

5.10.1. Government-Furnished Utilities. Electricity, water, sewage, air conditioning (AC), heating to the same extent it is furnished to government employees.

5.10.2. Telephone Services. The government will supply a class "A" office phones to all on base employees. At the Governments discretion, the government will provide ~~and one~~ a cell phone to selected contractor employees for official task order-oriented government business.

5.10.3. Custodial Service. The government will provide custodial service. The contractor will be required to perform general housekeeping procedures to maintain a clean work area.

5.11. **Security and Privacy**:

5.11.1. **Security**. The Contractor shall comply with all applicable security regulations and directives identified herein and other security requirements as shown elsewhere in this task order.

- This project is unclassified, but shall be managed as government proprietary. The software shall be protected from change except by specific authorization.
- Personnel are required to read, store, process sensitive information and operate/program sensitive database or equipment.
- The contractor shall ensure that all contractors assigned to this task understand and adhere to the Privacy Act of 1974.

- Access to sensitive (e.g., Privacy Act, FOUO material and classified) documents, data, records, etc., on government equipment must be consistent with DoD, Air Force, and MAJCOM directives and instructions. Private equipment may not be used to access or view classified material or privacy act data. (See AFI 33-112, AFI 33-200, AFMAN 33-223, AFSSI 8522 and AFSSI 8580.)
- Contractors must comply with all government security procedures and ensure security measures are in place to protect equipment and data from physical and virus damage, theft, loss, or access by unauthorized individuals. (See AFI 33-112, AFI 33-138, *Incident Response and Reporting*, AFI 33-200, *Information Assurance (IA) Management*, AFMAN 33-223, *Identification and Authentication*, Air Force Systems Security Instruction (AFSSI) 8502, *Organizational Computer Security*, AFSSI 8522, *Access to Information Systems*, and AFSSI 8580, *Remanence Security*).
- Below is a listing of some of the required annual training requirements of the Government:
  - DoD Information Assurance Awareness (ZZ133098) *[include if access to network]*
  - Information Protection (ZZ133078) *[include if on-site performance]*

5.11.2. **Data Integrity**. Data pertaining to other contracts and services reside on systems used by the AFRC. The contractor shall not divulge this information or use this information for the contractor's gain. In addition, any and all records, files, documents, and work papers, regardless of the type of media created in (i.e., physical, electronic, etc.) provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, *Management of Records*; AFI 33-364, *Records Disposition – Procedures and Responsibilities*; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable.

5.11.3. **Safeguarding Classified Information:**

5.11.3.1. The contractor shall comply with all security regulations and directives as identified herein and other security requirements as are shown elsewhere in this task order. The contractor shall comply with DD Form 254, **DoD Contract Security Classification**, attached to this task order.

5.11.3.2. The contractor shall conform to the provisions of *DOD 5220.22M, National Industrial Security Program Operating Manual (NISPOM),* DoD 5220.22-R, *Department of Defense Industrial Security Program*, DoD 5200.1-R, *Department of Defense Information Security Program* and AFI 31-401, *Air Force Information Security Program* , and AFI 31-601, *Industrial Security Program Management*. This is IAW with the performance of work under this task order shall be given access to classified information or material.

5.11.3. **Visitor Group Security Agreement (VGSA)**. The contractor shall enter into a visitor group security agreement. The agreement, shall comply with the provisions of all applicable AF and AFRC instructions. Coordination of the VGSA will be accomplished by the signatures of personnel identified on the coordination page.

5.11.4. **Clearances**. As a minimum, all contractors must have as a SECRET clearance. Certain positions, may in the future, may require a higher security clearance (i.e., TOP SECRET) in order to perform duties. These positions will be identified after award of this task order, if/when applicable. The majority of the work will be on government installations and facilities which require security clearances for access. The following items also apply:

- A NACLS Clearance is required.
- All personnel shall have an interim SECRET prior to employment.
- Certification Authority Workstation (CAW) requires a FINAL Secret prior to starting work.
- If a person is declined an appropriate clearance then they must be removed from the task.
- After DAA approval for connectivity to an Air Force network, the network administrators, system administrators, and organization computer managers will restrict access to the minimum necessary to fulfill defined mission requirements.

5.11.5. **Facility Clearances and Employee Clearance:**

5. 11.5.1. The contractor shall possess or obtain a facility clearance at the classification level of SECRET. The contractor shall obtain personnel security clearances on all employees who require unescorted entry into restricted areas, access to classified material, use of unclassified automated and classified information systems that have access to sensitive information (IT/AIS Level II), and access to the base network within 15 calendar days after receipt of the facility clearance or 60 days prior to performance start date if the contractor possesses a facility clearance. The government will conduct and assume all costs for personnel security investigations

5. 11.5.2. Contractor employees that require access to classified information or materials shall: (1) possess a valid and appropriate security clearance, (2) have executed an SF 312, **Non-disclosure Agreement**, and (3) have a valid need for access to the information to perform a lawful and authorized government function. This is in accordance with the performance of work under this task order and shall be authorized access to classified information or material. Contractor personnel are required to possess appropriate clearances prior to beginning work at the device locations.

5.11.6. **Employee Clearance/Investigations**. [Special Access Program (SAP) ONLY] Contract personnel shall possess a minimum of a SECRET clearance and have Special Access Program/Special Access Required (SAP/SAR) access with a privilege access of National Agency Check with Local Agency Check and Credit Check (NACLC) as mandated in DoD 5200.2-R, *DoD Personnel Security Program*, para C3.6.15 which defines the type of investigation required by each ADP (IT) level. Per DoDI 8500.2, *Information Assurance (IA) Implementation*, Table E3T.1., page 45 (civilian, military, and contractors) who require IA Administrator (with no IA Administrative Privileges) access to perform their duties must be coded as IT-II and therefore meet investigative requirements of NACLC. JAFAN 6/4 governs the minimum investigative requirements and periodic reinvestigation timeline for SAP access.

5.11.7. **Network Access**:

5.11.7.1. Network access is a privilege extended to contractor employees. It will be granted only after all criteria have been met and may be suspended for cause as defined in AFI 33-115V2, Section 5.6. Network access will be approved IAW AFI 31-501, *Personnel Security Program Management;* AFI 31-601; AFI 33-115V1, *Network Operations (Netops)*; AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*, **AFI 33-202**, AFMAN 33-223, *Identification and Authentication*; DoD 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, and DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*. Per AFI 33-115V2, "every individual who has access to the Air Force network (af.mil) domain, specialized systems and mission systems is a network user. Before becoming an AF network user, an individual must be trained and licensed. This process of training and licensing ensures that every Air Force network user is trained and aware of the basic principles of network security and their role in Information Assurance (IA)."

5.11.7.2. Every AF network user must possess a current and favorable National Agency Check with Written Inquires (NACLC) Investigation. Contractor personnel require a NACLC IAW para 5.11.3. above.

5.11.7.3. Foreign Nationals must meet the requirements of AF 31-501 prior to access. Access by Foreign Nationals must be processed and approved by the Foreign Disclosure Office (FDO) IAW AFSSI 8522, *Access to Information Systems*, para 3.2.1 and 3.2.3.

5.11.7.4. The Personnel Security Section (**Base or Wing/IPP**) will process and forward requests for Contractor NACLCs. The contractor will be notified by the (**Base or Wing/IPP**) Personnel Security section of the results of the NACLCs. The Personnel Security section will be the repository for the record of NACLCs conducted on Contractor employees for access to sensitive information and automated information systems.

5.11.7.5. Each Contractor employee requiring a NACLC shall submit to (**Base or Wing/IPP**) on copy of a completed SF85P, **Questionnaire for Public Trust Positions**. Information Protection personnel will fingerprint the Contractor employee on a FD Form 258, **Fingerprint Card**. To obtain an SF85P visit the U.S. General Services Administration GSA Forms Library web site at *http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?formType=SF* and download the Form.

5.11.7.6. Upon completion of the subsequent investigation suitability of employment review, **(Base or Wing/IPP**) will notify the unit Commander (or designee) of the organization for employee receiving a favorable/unfavorable NACLC by forwarding a copy of the Record of Employment Suitability Form. The Contracting Officer will notify the Contractor of employees receiving a favorable/unfavorable NACLC by forwarding a copy of the Record of Employment Suitability Form to the Contractor. The Contractor's employee(s) will not be allowed access to sensitive information or restricted areas when the current NACLC is unfavorable.

5.11.7.7. When the Government is in the process of conducting a NACLC investigation on a Contractor employee and that individual's employment is terminated before the investigation is completed, the Contractor shall immediately forward to **(Base or Wing/IPP)** written notice of the termination.

5.11.7.8. Pending favorable NACLC's contractor employees shall work in restricted areas only with government escorts. When the Government is in the process of conducting a NACLS investigation, and that individual's employment is terminated before the investigation is completed, the contractor shall immediately forward a written notice of the individual's termination to the Personnel Security Section

5.11.8. **Contractor Access to Air Force Installations**:

5.11.8.1. The contractor shall obtain base identification, if required, for all contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the task order. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished, contractor identification badges while visiting or performing work on the installation.

5.11.8.2. The contractor shall submit a written request on company letterhead to the contracting officer listing the following: task order number, location of work site, start and stop dates, and names of employees and subcontractor employees needing access to the base. The letter will also specify the individual(s) authorized to sign for a request for base identification credentials or vehicle passes. The contracting officer will endorse the request and forward it to the issuing base pass and registration office or security police for processing. When reporting to the registration office, the authorized contractor individual(s) should provide a valid driver's license, current vehicle registration, and valid vehicle insurance certificate to obtain a vehicle pass.

5.11.8.3. During performance of the task order, the contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials for any employee who no longer requires access to the work site.

5.11.8.4. When work under this task order requires unescorted entry to controlled or restricted areas, the contractor shall comply with AFI 31-209 citing the appropriate paragraphs as applicable.

5.11.8.5. Upon completion or termination of the task order or expiration of the identification passes, the prime contractor shall ensure that all base identification passes issued to employees and subcontractor employees are returned to the issuing office.

5.11.8.6. Failure to comply with these requirements may result in withholding of final payment.

5.11.9. **Physical Security**:

5.11.9.1. **Mission Essential Services.** Contractor services provided under this task order are designated as non-mission essential IAW DoDI 3020.37. The contractor is to be aware of the discontinuance of PWS requirements during a crisis situation. The contractor personnel shall follow agency procedures to identify and safeguard reports and data accordingly. The contractor shall ensure that contractor personnel assigned to this requirement are briefed annually on properly identifying and handling Privacy Act data and reports.

5.11.9.1. Installation Perimeter Access Control. The requirements for installation perimeter access are detailed in Air Force Federal Acquisition Regulation Supplement (AFFARS) clause 5352.242-9000 entitled, *Contractor Access to Air Force Installations*, in Section I, *Contract Clauses*, of the basic task order.

5.11.9.2. Resource Protection and Integrated Defense. The Contractor shall safeguard all government property in accordance with AFI 31-101, *Integrated Defense*, and any forms provided for Contractor use. The Contractor shall immediately report all thefts, vandalism, or destruction of property and equipment (Government or Contractor owned) to the AFRC/A6 Directorate Security Manager or Alternate Security Manager and the Contracting Officer Representative (COR).

5.11.9.3. **Information Security:**

5.11.9.3.1. **Unclassified Information Security.** The Contractor shall handle and safeguard Controlled Unclassified Information in accordance with DoD Manual 5200.1-M, Volume 4 entitled, *DoD Information Security Program: Controlled Unclassified Information (CUI)*.

5.11.9.3.2. **Information Protection Program.** The Contractor shall participate in the host installation's Information Protection Program (IPP).

5.11.10. **Privacy Act**. Work on this project requires that personnel have access to Privacy Act information. Personnel shall adhere to the Privacy Act of 1974, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations. The contractor personnel shall follow agency procedures to identify and safeguard reports and data accordingly. The contractor shall ensure that contractor personnel assigned to this requirement are briefed annually on properly identifying and handling Privacy Act data and reports.

5.11.11. **Common Access Cards (CACs) for Contractor Personnel**:

5.11.11.1. For installation(s)/location(s) cited in the task order, contractors shall ensure Common Access Cards (CACs) are obtained by all contract or subcontract personnel who meet one or both of the following criteria:

5.11.11.1.1. Require logical access to Department of Defense computer networks and systems in either:

5.11.11.1.1.1. The unclassified environment; or

5.11.11.1.1.2. The classified environment where authorized by governing security directives.

5.11.11.1.2. Perform work which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

5.11.11.2. Contractors and their personnel shall use the following procedures to obtain CACs:

5.11.11.2.1. Contractors shall provide a listing of personnel authorized a CAC to the contracting officer. The contracting officer will provide a copy of the listing to the government representative in the local organization designated to authorize issuance of contractor CACs (i.e., “authorizing official”).

5.11.11.2.2. Contractor personnel on the listing shall each complete and submit a DD Form 1172-2, **Application for Identification Card/DEERs Enrollment**, or other authorized DoD electronic form to the authorizing official. The authorizing official will verify the applicant’s name against the contractor’s listing and return the DD Form 1172-2 to the contractor personnel.

5.11.11.2.3. Contractor personnel will proceed to the nearest CAC issuance workstation (usually the local Military Personnel Flight (MPF) with the DD Form 1172-2 and appropriate documentation to support their identification and/or citizenship. The CAC issuance workstation will then issue the CAC.

5.11.11.3. While visiting or performing work on installation(s)/location(s), contractor personnel shall wear or prominently display the CAC as required by the governing local policy.

5.11.11.4. During the performance period of the task order, the contractor shall:

5.11.11.4.1. Within 7 working days of any changes to the listing of the task order personnel authorized a CAC, provide an updated listing to the contracting officer who will provide the updated listing to the authorizing official;

5.11.11.4.2. Return CACs in accordance with local policy/directives within 7 working days of a change in status for contractor personnel who no longer require logical or physical access;

5.11.11.4.3. Return CACs in accordance with local policy/directives within 7 working days following a CACs expiration date; and

5.11.11.4.4. Report lost or stolen CACs in accordance with local policy/directives.

5.11.11.5. Within 7 working days following completion/termination of the task order, the contractor shall return all CACs issued to their personnel to the issuing office or the location specified by local policy/directives.

5.11.11.6. Failure to comply with these requirements may result in withholding of final payment.

5.11.12. **Specific Instruction for HQ AFRC CAC Processing**. Common Access Card (CAC) Issue Procedures. Every contractor, regardless of which location they work at, will be required to have a CAC in order to access the network. With that said, the procedures for the issuance of CACs will be as follows:

5. 11.12.1. The Vendor Program Manage will verify the individual has a security clearance.

5. 11.12.2. Once verified, the Vendor Program Manage will complete the Trusted Agent Authorization to Issue Common Access Card (CAC). (See Table 8)

5. 11.12.3. The completed form will either be hand-carried over to the COR or scanned and sent via email to the COR in .pdf format. NOTE: The letter shall be legible to the COR; anything considered not legible, will be returned back to the vendor for correction and resubmittal.

5.11.12.4. The COR will sign the letter and input the information into the Contractor Verification System (CVS)/Trusted Associate Sponsorship System (TASS) database.

5. 11.12.5. Once inputted into the CVS/TASS database, the COR will notify the individual (contractor requiring the CAC) by email. Once notified, the contractor will have 7 days to access the website and provide the information required. If not accomplished within 7 business days, the request will automatically be deleted from the CVS database and the contractor will have to start the process over (See para 5.11.13.3.).

5. 14.15.6. Once the contractor has completed all requirements, then the COR will be notified via email to go into the CVS/TASS database and approve the CAC application. Once the COR approves the CAC request, the contractor will be notified via email that the CAC application was approved and then will be allowed to report to the nearest Military Personnel Flight to get issued their CAC.

5.11.13. **AFRC Building Badge Issue Procedures (Robins AFB, GA ONLY)**. If a contractor is scheduled to work in the HQ AFRC Building, they will be required to have a building badge in order to access the building. With that said, the procedures for the issuance of an AFRC Badge will be as follows:

5.11.13.1. Newly assigned personnel, to include contractors, will in-process through the Contractor's Functions Security Officer (FSO) and in-process through the AFRC/A6 Security Manager.

5.11.13.2. The Contractor FSO will ensure members have the required personnel security investigation and clearance needed to perform officially assigned duties.

5.11.13.3. The Contractor's FSO will then submit a JPAS visit request to the AFRC Information Protection Office (AFRC/IPO). The Contractor FSO needs to ensure that the Security Management Office (SMO) Code reflects RX0MFCMF).

5.11.13.4. Once the AFRC/IPO has validated the JPAS visit request, the individual contractor will be sent to the AFRC Information Protection Office (AFRC/IPO) (Bldg 220) and issued a building badge.

5.11.13.5. In the event a contractor requires access to additional controlled areas within the HQ AFRC building, the contractor will contact the AFRC/A6 Security Manager. The Security manager will complete an AF Form 2586, Unescorted Entry Authorization Certificate, have the appropriate coordinating official sign and then have the controlled area added to the building badge.

5.11.13.6. Contractor access at assigned to other Reserve Host Bases. If the contractor requires access to controlled area(s) within other Reserve Host Bases of assignment, the contractor will contact the Base Security Manager and follow the local procedures of the issuance of building badges and/or access to controlled areas, if required.

5.11.14 Contractor Manpower Reporting (via eCMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the AFRC Headquarters and Enterprise IT Services via a secure data collection site. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil.

Reporting inputs will be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported any time during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to the CMRA help desk.

5.11.14.1 Reporting Period: Contractors are required to input data by 31 October of each year.

5.11.14.2. Uses and Safeguarding of Information: Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data.

5.11.14.3. User Manuals: Data for Air Force service requirements must be input at the Air Force CMRA link. User manuals for government personnel and contractors are available at the Army CMRA link at http://www.ecmra.mil.

5.12. **Standards and References**. Hardware and software manuals for systems supported under this task order will be made available and shall remain property of the government.

5.13. Schedule and Delivery Instructions:

The specific deliverables and schedule for delivery shall be per the performance/Deliverables Matrix. The COR reserves the right to prioritize work and negotiate any changes in delivery dates.

Unsatisfactory Work – Performance by the contractor to correct defects identified by the Government as a result of quality assurance surveillance and by the contractor as a result of quality control shall be at the contractor’s own expense without additional reimbursement by the Government.

The acceptance of deliverables and satisfactory work performance required herein shall be based on the standards as specified in the requirements per Section 2 of this document. The COR will review the contractor's performance indicators IAW all the specifications stated in this document. Only the COR or authorized alternate has the authority to inspect, accept, or reject work performed under this task order.

5.14. **Quality Control Plan (QCP)**. In compliance with standards as specified in the requirements per Section 2 of this document, the contractor shall provide and maintain a Quality Control Plan (QCP) that contains, as a minimum, the items listed in 5.16. to the Contracting Officer (CO) for acceptance not later than (NLT) five (5) work days after the start of this task order. The CO will notify the contractor of acceptance or required modifications to the plan within five (5) work days. The contractor shall make appropriate modifications and obtain final acceptance of the plan by the CO within five (5) work days of notification of required changes.

5.14.1. The plan shall include the following minimum requirements:

- A description of the inspection system to cover all services listed in the Performance/Deliverables Matrix. Description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title and organizational placement of the inspectors. Additionally, control procedures for any government provided keys or lock combination should be included.
- A description of the methods to be used for identifying and preventing defects in the quality of service performed.
- A description of the records to be kept to document inspections and corrective or preventive actions taken.
- All records of inspections performed shall be retained and made available to the government upon request throughout the task order period of performance, and for the period after task order completion, until final settlement of any claims under this task order.

5.15. **Quality Assurance**. The Government will evaluate the contractor's performance of this task order. For those services listed in the Performance/Deliverables Matrix, the COR, or evaluators will follow the method of surveillance specified in this task order. Government personnel will record all surveillance observations. When an observation indicates defective performance, the COR, or evaluators will require the task order manager or representative at the site to initial the observation. The initialing of the observation acknowledges that he or she has been made aware of the defective performance and does not necessarily constitute concurrence with the observation. Government surveillance of services not listed in the Performance/ Deliverables Matrix or by methods other than those listed in the Performance/Deliverables Matrix (such as provided in the Inspection of Services clause) may occur during the performance period of this task order. Such surveillance will be done according to standard inspection procedures or other task order provisions. Any action taken by the CO as a result of surveillance will be according to the terms of this task order.

5.15.1. **CPARS/Past Performance.** The Government will provide and record Past Performance Information for acquisitions over $150,000 utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS process allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

Contractors are required to register in the CPARS, so contractor's may review and comment on past performance reports submitted through the CPARS.

Contractors are required to register at the following web sites and confirm via email with the

CAM completion of the registration process:

CPARS: https://www.cpars.csd.disa.mil/
PPIRS: http://www.ppirs.gov

5.16. **Performance/Deliverables Metrics**:

Performance Standard	PWS Ref	AQL	Method of Surveillance
Provide accurate/comprehensive MTS and MFS reports within 10 work days after end of month	1.4.4 & 1.4.5	On-time delivery at 100% level	100% Inspection of MTS/MFS reports
Ensure NIPR/SIPR CAT vulnerabilities for each server/ workstation does not exceed AFRC, AF, DISA, or DoD standards	2.3, 2.3.2.10, & 2.4	Must be ≤2.49 vulnerabilities per each server/ workstation	100% inspection of monthly Gov't scans; 100% inspection of data reported in metrics
Provide AFNet Support Element (ASE) and MAJCOM Support Element (MSE) deliverables	2.3.1 thru 2.3.2	Provide status update within 5 work days after the end of each month	Periodic Inspection
Provide project milestones, metrics, plans and progress for assigned projects on a monthly basis or as requested by the Government	2.3.1 thru 4.9	On time delivery at 100% level; accurate and correct format	Periodic Inspection through MTS
Provide Communications Focal Point (CFP) Support	2.3.3	By the first business day of the week, ≤50 unresolved tickets in the queue for the previous week	Periodic Inspection; weekly Remedy Reports

Performance Standard	PWS Ref	AQL	Method of Surveillance
Provide Communications Focal Point (CFP) Support	2.3.3	≤85% of all tickets that were closed during the week were not open longer than 14 days	Periodic Inspection; weekly Remedy reports
Provide comprehensive monthly telephone metrics report tracking number of calls, responses, etc… within 5 work days after end month	2.5.1.11 and 2.5.2.8	On-time delivery at 95% level	Periodic Inspection of Telephone Reports
Maintain telephone system up-time rate	2.5.1.11 and 2.5.2.8	≥98%	Periodic Inspection of Telephone Reports
Provide comprehensive VTC usage report on a bi-weekly basis	2.5.3.2	On-time delivery at 100% level	Periodic Inspection
Ensure the Service Oriented Cloud Environment (SOCE) system is available 24/7	2.5.6.3.1.3 and 2.5.6.4.3	99.9%	Periodic Inspection
IT Requirements Support Deliverables	4.2.3	On-time delivery at 100% level, as directed by the Government	Periodic Inspection of deliverables
Provide site survey reports, VOIP installation and reliability metrics, and/or program updates, as required	4.3.2	On-time delivery at 100% level	Periodic Inspection of reports
Provide/present ICM status reports and ICM program updates, as required	4.5.2	On-time delivery at 100% level	Periodic Inspection of reports
Provide VTC usage metrics on a quarterly basis	4.6.1	On-time delivery at 100% level	Periodic Inspection of metrics
Deliver Annual Operating Plan within 60 days of beginning of period of performance, with quarterly updates thereafter	4.7.9.1	On-time delivery at 100%	100% inspection
Annual Operating Plan schedules/ milestones as approved by Government	4.7.9.1	On-time delivery at 100% within 30 days of schedule	100% inspection
Provide Cyber Force Readiness deliverables/assigned tasks within 5 working days or unless otherwise directed by the	4.22	On-time delivery at 100% level; accepted by Government	100% Inspection

Performance Standard	PWS Ref	AQL	Method of Surveillance
Government			
Provide Cyber Force Readiness with updated metrics and demographics for functional managers	4.22	On-time delivery at 95% level within 7 working days	100% Inspection
Provide Cyber Force Readiness with new metrics and demographics for functional managers	4.22	On-time delivery at 95% level within 14 working days	100% Inspection
Provide Cyber Force Readiness fill rates for scheduled Cyber 200/300 classes	4.22	Provide accurate/ comprehensive Cyber Force Readiness fill rates for Cyber 200/300 classes by the 5th business day each month	100% Inspection
Provide updates to the Content Master Calendar guide and business rules, status reports, and metrics, as required.	4.23.2	100% complete, current and accurate at all times	Periodic Inspection

5.17. **Personal Services**:

GSA will not issue orders to provide personal services. Administration and monitoring of the contractor's performance by GSA or the COR shall not be as detailed or continual as to constitute supervision of contractor personnel. Government personnel may not perform any supervisory functions for contractor personnel, such as interviewing, appraising individual performance, scheduling leave or work, or directing how to perform work.

GSA meets the needs of its clients for information technology support through non-personal services task order. To counter the circumstances that infer personal services and to preserve the non-personal nature of the task order, the contractor shall adhere to the following guidelines in the performance of the task:

- Provide for direct supervision of all contract employees assigned to the task.
- Refrain from discussing the issues such as skill levels and hours, salaries, cost and funding data, or administrative and personnel matters affecting contractor employees with the client.
- Ensure close communication/coordination with the GSA Information Technology Project Manager, reporting problems to the as they occur (not waiting for a monthly meeting).
- Do not permit Government officials to interview potential contractor employees, discuss individual performance, approve leave or work scheduling of contractor employees,

terminate contractor employees, assist contractor employees in doing their jobs or obtain assistance from the contractor in doing Government jobs.

- Do not assign contractor personnel to work under direct Government supervision.
- Maintain a professional distance from Government employees.
- Provide contractor employees with badges, if appropriate, identifying them as contractors.
- Ensure proper communications with the Government. Technical discussion and government surveillance is acceptable, but the Government cannot tell the contractor how to do the job.
- Assign a task leader to the task order. The task leader or alternate should be the only one who accepts tasking from the assigned Government point of contact or alternative.
- Use work orders to document and manage the work and to define the details of the assignment and its deliverables. The Government has the right to reject the finished product or result and this does not constitute personal services.
- When travel is required for the performance on a task, contractor personnel are only to travel as directed by their contract management.

5.18. **Compliance Documents.** The Contractor shall comply with the latest edition of the following directives, instructions, regulations, manuals and statutes. (See Table 2 for a list of all publications and forms.)

5.19. **Invoices:**

5.19.1. Payment Information. The contractor shall provide the following payment information for GSA use. It must be an exact match with the information under the task order number in the ITSS Contract Registration as well as with the information under the contractor's Data Universal Numbering System (DUNS) number in the Central Contractor Registration (CCR), http://www.ccr.gov. Mismatched information could result in rejected purchase orders and payments.

- Legal Business Name/DBA (Doing Business As)
- Physical Address
- Remittance Address
- Employer's Identification Number (Federal Tax ID)
- DUNS

5.19.2. Invoices shall be submitted monthly on official company letterhead as follows:

- GSA Account Number
- GSA Task Order Number
- Period of Performance for the Billing Period
- Point of Contact and Phone Number
- Total Invoice Amount
- Prompt Payment Discount Offered, if applicable

- Charges, identified by Deliverable or Customer Line Item Number (CLIN), with a narrative description of the service performed
- Total cumulative Task Order Amount and Burn Rate
- Subtasks will be separated and reported on the invoices.

5.19.3. The amount invoiced must include the following information:

- Skill Level Name
- Skill Level Number Assigned on the GSA Schedule or Government Wide Acquisition Contracts (GWAC)
- Actual Hours Worked during the Billing Period (for consultant only)
- Travel, if applicable
- Training, if applicable
- Other Direct Costs, if applicable

5.19.4. Contractor must submit an acceptance document and attach a copy of the invoice to GSA IT Solutions Shop (ITSS) web-based Order Processing System (https://portal.fas.gsa.gov/web/guest) or future equivalent. The COR and GSA Contracting Representative must approve the invoice in ITSS prior to payment.

5.19.5. **{RESERVED}** ~~**The original invoice must be submitted to GSA's finance center at the same time that it is entered into ITSS in order for a match to occur for payment. This may be done electronically to the finance center web site (http://www.finance.gsa.gov) or via regular U. S. mail to this address:**~~

~~**General Services Administration**~~
~~**Greater Southwest Finance Center**~~
~~**Accounts Payable Br – 7BCP**~~
~~**Fund 299X**~~
~~**P. O. Box 17181**~~
~~**Fort Worth, TX 76102-0181**~~

~~**Failure to comply with paragraphs 5.19.4. and 5.19.5. will result in an automatic rejection.**~~

5.19.6. All reimbursable costs must not exceed the limit(s) specified in the task order. The Government will not pay charges that are not specifically identified in the task and approved, in advance, by the Government. Copies of receipts, travel vouchers, etc. that have been completed IAW Government Joint Travel Regulations (JTR) shall be attached to the invoice to support charges other than employee labor hours. Original receipts shall be maintained by the contractor and made available to Government auditors upon request.

5.19.7. Payment Schedule. The contractor shall invoice for work performed the prior month. Invoice shall be submitted every month, no later than the 10th of each month.

5.19.8. Invoices for final payment must be so identified and submitted within 60 days from task completion. No further charges are to be billed. The contractor shall request an extension for final invoices that may exceed the 60 days from GSA.

5.20. **Compliance with Section 508** (if applicable). All electronic and information technology (EIT) procured through this task order must meet the applicable accessibility standards at 36 Code of Federal Regulations (CFR) 1194, unless an agency exception to this requirement exists. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at http://www.access-board.gov/sec508/508standards.htm. The contractor shall indicate for each line item in the schedule whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the proposal must indicate where full details of compliance can be found (e.g., vendor's website or other specific location).

5.21. **GSA Specific** (as applicable). The following FAR clauses apply:

5.21.1. **52.217-8, *Option to Extend Services***. The Government may require continued performance of any services within the limits and at the rates specified in the task order. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

5.21.2. **52.217-9, *Option to Extend the Term of the Task Order***:

(a) The Government may extend the term of this task order by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the task order expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended task order shall be considered to include this option clause.

(c) The total duration of this task order, including the exercise of any options under this clause, shall not exceed 5 years and 6 months

5.21.3. **52.232-18, *Availability of Funds***.

5.21.4. **52.232-22, *Limitation of Funds***.

5.21.5. Clauses incorporated by reference: Defense Federal Acquisition Regulation Supplement (DFARS) Clauses:

- **252-203-7001, *Prohibition on Persons Convicted of Fraud or Other Defense-Contract Related Felonies* (Dec 2004) (applicable if non-commercial)**
- **252.203-7002, *Display of DoD Hotline Poster* (Dec 1991)**
- **252.204-7000, *Disclosure of Information* (Dec 1991)**
- **252.204-7003, *Control of Government Personnel Work Product* (Apr 1992)**
- **252.204-7004, *Alternate A, Central Contractor Registration* (Sep 2007)**

(substitute for paragraph (a) of FAR 52.204-7, if included)

- **252.204-7005, *Oral Attestation of Security Requirements* (Nov 2001) (Applicable if FAR 52.204-2 included)**
- **252.204-7007 *Alternate A, Annual Representations and Certifications* (Jan 2008) (Applicable if FAR 52.204-8 included)**
- **252.205-7000, *Provision of Information to Cooperative Agreement Holders* (Dec 1991)**
- **252.206-7000, *Domestic Source Restriction* (Dec 1991) (Applicable if restricted to domestic sources under the authority of FAR 6.302-3)**
- **252.209-7001, *Disclosure of Ownership or Control by the Government of a Terrorist Country* (Oct 2006)**
- **252.209-7002, *Disclosure of Ownership or Control by a Foreign Government* (Jun 2005) (applicable if access to “proscribed information” (defined in clause) is needed for task order performance)**
- **252.209-7004, *Subcontracting with Firms That Are Owned or Controlled by the Government of a Terrorist Country* (Dec 2006)**
- **252.211-7007, *Item Unique Identification of Government Property* (Sep 2007) (applicable if FAR 52.245-1 or 52.245-2 included)**
- **252.212-7000, *Offeror Representations and Certifications—Commercial Items* (Jun 2005) (applicable if commercial exceeding Simplified Acquisition Threshold)**
- **252.212-7001, *Contract Terms and Conditions Required to Implement Statutes or Executive Orders Applicable to Defense Acquisitions of Commercial Items* (Apr 2007) (applicable if commercial)**
- **252.215-7000, *Pricing Adjustments* (Dec 1991) (Applicable if FAR 52.215-11, 52.215-12 or 52.215-13 included)**
- **252.215-7002, *Cost Estimating System Requirements* (Dec 2006) (Applicable if awarded on the basis of cost or pricing data)**
- **252.215-7003, *Excessive Pass-Through Charges – Identification of Subcontract Effort* (Apr 2007) (applicable unless award was FFP w/ Price Competition, FFP-EPA w/ Price Competition, FFP Commercial, or FFP-EPA Commercial)**
- **252.216-7002 *Alternate A, Time and Materials/Labor-Hour Proposal Requirements – Non-Commercial Item Acquisition with Adequate Price Competition* (Feb 2007) (applicable if contemplating T&M or LH for Non-commercial with price expected to be based on adequate price competition)**
- **252.219-7003, *Small Business Subcontracting Plan* (DoD Contracts) (Apr 2007) (applicable if FAR 52.219-9 included)**
- **252.223-7004, *Drug-Free Work Force* (Sep 1998)**
- **252.223-7006, *Prohibition on Storage and Disposal of Toxic and Hazardous Materials* (Apr 1993)**
- **252.225-7000, *Buy American Act –Balance of Payments Program Certificate* (Jun 2005) (use instead of FAR 52.225-2 if included)**
- **252.225-7012, *Preference for Certain Domestic Commodities* (Jan 2007)**
- **252.225-7031, *Secondary Arab Boycott of Israel* (Jun 2005)**
- **252.226-7000, *Notice of Historically Black College or University and Minority Institution Set-Aside* (Apr 1994) (applicable if set-aside for HBCU/MI)**

- **252.226-7001,** ***Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns*** **(Sep 2004) (use for supplies or services exceeding $500,000 in value)**

5.21.6. **52.222-2,** ***Payment for Overtime Premiums***

(a) The use of overtime is authorized under this task order if the overtime premium does not exceed **xxxxx** or the overtime premium is paid for work:

(1) Necessary to cope with emergencies such as those resulting from accidents, natural disasters, breakdowns of production equipment, or occasional production bottlenecks of a sporadic nature;

(2) By indirect-labor employees such as those performing duties in connection with administration, protection, transportation, maintenance, standby plant protection, operation of utilities, or accounting;

(3) To perform tests, industrial processes, laboratory procedures, loading or unloading of transportation conveyances, and operations in flight or afloat that are continuous in nature and cannot reasonably be interrupted or completed otherwise; or

(4) That will result in lower overall costs to the Government.

(b) Any request for estimated overtime premiums that exceeds the amount specified above shall include all estimated overtime for task order completion and shall:

(1) Identify the work unit; e.g., department or section in which the requested overtime will be used, together with present workload, staffing, and other data of the affected unit sufficient to permit the Contracting Officer to evaluate the necessity for the overtime;

(2) Demonstrate the effect that denial of the request will have on the contract delivery or performance schedule;

(3) Identify the extent to which approval of overtime would affect the performance or payments in connection with other Government task orders, together with identification of each affected task order; and

(4) Provide reasons why the required work cannot be performed by using multi-shift operations or by employing additional personnel.

NOTE: Some DFARS clauses may apply;

DFAR 252.232-7007 LIMITATION OF GOVERNMENT'S OBLIGATION (MAY 2006)

(a) Task order line items **1.2.** through **8.2.,** with the exception of **2.3.11**., of the PWS are incrementally funded. For these item(s), the sum of **TBD** of the total price is presently available for payment and allotted to this task order. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the task order. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the task order for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the

Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer, in writing, at least 90 days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the task order for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this task order entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the task order line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of task order performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the task order will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the task order line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the task order line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the task order line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the task order is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this task order pursuant to the clause of this task order entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this task order IAW the following schedule: (Estimated)

On execution of task order	$ TBD
(September) (01), (2012)	$ TBD
(September) (01), (2013)	$ TBD
(September) (01), (2014)	$ TBD
(September) (01), (2015)	$ TBD

252.237-3 Continuity of Services.

DFARS 252.209-7999 REPRESENTATION BY CORPORATIONS REGARDING AN UNPAID DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (DEVIATION 2012-00004) (JAN 2012)

(a) In accordance with sections 8124 and 8125 of Division A of the Consolidated Appropriations Act, 2012,(Pub. L. 112-74) none of the funds made available by that Act may be used to enter into a task order with any corporation that—

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that—

(1) It is [ ] is not [X] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability,

(2) It is [ ] is not [X] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months. (End of provision)

5.22. The following definitions and descriptions apply:

- "**Client On-Site Lead (Government Site Lead – QA at a particular base)"** is the inherently governmental Quality Assurance Representative at each location who is responsible for ensuring the contractor is performing all said duties at the particular location (base). This is normally the CS/CF commander and/or his/her Senior ART.
- "**Contracting Officer**" is the GSAs appointed representative who has the overall responsibility for the management of this task order.
- "**Contractor**" includes the prime contractor, parent company, affiliates, divisions, and subsidiaries.

- "**Contracting Officer Representative (COR)"** is the individual is responsible for looking out for the best interests of the government in regards to this task order.
- "**Development**" includes all efforts toward solution of broadly defined problems. This may encompass research, evaluating technical feasibility, proof of design and test, or engineering of programs not yet approved for acquisition or operation.
- "**Mashup**" is an application that uses and combines data, presentation or functionality from two or more sources to create new services. The term implies easy, fast integration, frequently using open APIs and data sources to produce enriched results that were not necessarily the original reason for producing the raw source data. The main characteristics of the mashup are combination, visualization, and aggregation.
- "**On-Site Project Manager**" is the individual contractor who has the overall responsibility for the day-to-day management of this task order. This individual will be the one assigned locally (to the Robins AFB, GA vicinity) that makes all the on-site decisions in regards to this task order.
- "**Ontology**" is a formal representation of a set of concepts, and the relationships between those concepts. Ontologies give us a standard method for capturing the meaning of complex systems and their capabilities.
- "**Proprietary Information**" includes all information designated as proprietary IAW law and regulation, and held in confidence or disclosed under restriction to prevent uncontrolled distribution. Examples include limited or restricted rights data, trade secrets, sensitive financial information, and computer software. Proprietary information may appear in technical data, cost and pricing data, or may involve classified information. For the purpose of this definition, proprietary information pertains to both contractor and Government information.
- "**System**" means the group of related items that is the subject of acquisition or management, for which support has been ordered under this task order.
- "**Systems Engineering**" means a combination of substantially all of the following activities: determining specifications, identifying and resolving interface problems, developing test requirements, evaluating test data, and supervising design.
- "**System Life**" means all phases of the system development, production, or sustainment.
- "**Technical Direction**" includes a combination of substantially all of the following activities: developing work statements, determining parameters, directing other contractors' operations, and resolving technical controversies.
- "**Vendor Site Lead**" is the individual contractor who has the overall responsibility for the day-to-day management of this contract at their particular site (base). This individual makes all on-site decisions in regards to the management of this contract.

5.23. Inclement Weather. There will be times when inclement weather will impact a base and/or organization (i.e., snow storm, flooding, etc.) in such a way that it will become a safety concern. When this happens and the Wing/Base Commander closes a base, the contractor shall adhere to all directives of the military installation. When it comes to pay issues for time and material contractor support, the contractor shall only bill the Government for hours worked.

5.24. Federal Holidays. The contract shall not have staff present at the government installation facilities on federal holidays. The federal holidays observed are as follows: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day and Christmas Day.

5.25. Family, Energy Conservation, and Early Release Days. There will be days when the Government, MAJCOM, and/or Base Commander will direct Family Days, Energy Conservation Days, and/or early release days. When these days are identified, the contractor is expected to work when the facilities are available for them to do so. Furthermore, the COR can inform contractors regarding the level of performance expected for the particular day(s), but may not direct the contractor regarding whether or not to compensate employees if not required to work that day. The Service Contract Act does not require contractor employees to be paid for time if they do not work. The contractor may elect to grant employees the day off with pay, but there is no additional Government task order costs (wages for these hours are already in the task order cost). This task order specifies that in order for contractors to remain in place, they must have government oversight in place.

5.26. Safety:

5.26.1. **Health & Safety Program.** The Contractor is responsible for the safety and health of their personnel and protection of the public on Government work sites (DODI 6055.1, Paragraph E5.1). The Contractor shall maintain a health and safety program that meets OSHA standards. If the CO notifies the Contractor of a potential OSHA violation, the Contractor is obligated to comply with the applicable OSHA regulations.

5.26.2. **Incident or Mishap Procedures.** The contractor shall immediately call 911. The Contractor shall within one (1) hour notify the COR/CO and Government Safety Manager of all mishaps or incidents at or exceeding $2,000 (material + labor) for damage to government property. This notification requirement shall also include physiological mishaps/incidents. A written or email copy of the mishap/incident notification shall be sent within three (3) calendar days to the COR who will forward to the Government Safety Manager. For information not available at the time of initial notification, the Contractor shall provide the remaining information not later than twenty (20) calendar days after the mishap, unless extended by the COR/CO. Mishap notifications shall contain, as a minimum, the following information:

- Task order, task order number, name and title of person(s) reporting
- Date, time and exact location of accident/incident
- Brief narrative of accident/incident (events leading up to the accident/incident)
- Cause of accident/incident (if known)
- Estimated cost of accident/incident (material + labor to repair/replace)
- Nomenclature of equipment and personnel involved in the accident/incident
- Corrective actions (taken or proposed)
- Other pertinent information

The Contractor shall, in the event of an accidental incident/mishap, take reasonable action to establish control of the incident/mishap scene, prevent further damage to persons or property, and preserve evidence until released by the incident/mishap investigative authority.

5.26.3. **Fire Emergencies.** The Contractor personnel shall dial 911 to report fire related emergencies.

5.26.4. **Department of Labor Inspection of Contractor Operations.** The Contractor is subject to Department of Labor (DoL) inspections and enforcement by OSHA health and safety officials while performing work on a Government installation. The OSHA health and safety officials may access workplaces on Government installations at any time, scheduled or unscheduled, during regular work hours. The OSHA health and safety officials must meet security requirements to enter restricted or classified areas. The Contractor shall notify the COR/CO upon notification of a visit.

5.26.5. **Fire Prevention Training.** The contractor personnel who work on a government installation shall participate in fire extinguisher training in accordance with AFI 91-203, paragraphs 6.2.1, 6.2.16 and 6.2.17.

5.26.6. **Fire Protection and Prevention Program.** All contractor personnel performing work on properties under jurisdiction of the Government shall be responsible for fire safety and compliance with all applicable OSHA, State, Air Force, AFRC, and base regulations and directives. The contractor personnel shall attend a contractor's briefing on fire safety prior to any work. The contractor shall ensure that all contractor personnel and sub-contractors under their control are briefed on fire prevention practices in accordance with applicable directives. The contractor personnel are required to take annual fire prevention refresher training in accordance with RAFBI 32-2001, paragraph 2.4.

APPENDIX

TABLE 1
ACRONYMS AND ABBREVIATIONS

24/7	24 hours-a-day/7 days a week
24 AF	24th Air Force
38 EIG	38th Engineering Installation Group
951 RSPTS	951st Reserve Support Squadron
AC	Air Conditioning
ACART™	Architecture Compliance and Requirements Traceability
ACC	Air Combat Command
ACO	Acquisition Accounting Officer
ACP	Allied Communications Publication
AD	Active Directory
AFB	Air Force Base
AFCAP	Air Force Certification and Accreditation Program
AFDS	Air Force Directory Services
AFFARS	Air Force Federal Acquisition Regulation Supplement
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFMSS	Air Force Mission Support System
AFNET	Air Force Network
AFPEO	Air Force Program Executive Office
AFRC	Air Force Reserve Command
AFRISS-R	Air Force Recruiting Information Support System–Reserve
AFSPC	Air Force Space Command
AFSSI	Air Force Systems Security Instruction
AIM	Asset Inventory Management
AIS	Automated Information Systems
AMC	Air Mobility Command
AMS	Automated Metric Set
ANSI	American National Standards Institute
AO	Accountable Officer
AoA	Analysis of Alternatives
AQL	Accepted Quality Level
ARB	Air Reserve Base
AROWS-R	Air Force Reserve Orders Writing System-Reserve
ARS	Air Reserve Station
ASE	AFNet Support Element
A/V	Audio/Visual
AV1	All Views 1
AW	Airlift Wing
BAR	Basing Action Request
BCL	Business Capabilities Lifecycle
BEA	Business Enterprise Architecture

BES	Blackberry Enterprise Server
BIP	Basic Image Profile
BPR	Business Process Re-engineering
BRI	Basic Rate Interface
BRM	Business Reference Model
C2	Command and Control
C2IPS	Command and Control Information Processing System
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISP	Command Control Communications Computers Integrated Support Plans
C&A	Certification and Accreditation
C&I	Communications and Information
CAC	Common Access Card
CAF	Contractor Access Fees
CAM	Customer Account Manager
CAS	Client Access Server
CAW	Certification Authority Workstation
CBT	Computer Based Training
CCI	Controlled Cryptographic Items
CCNA	Cisco Certified Network Associate
CCR	Central Contractor Registration
CFR	Code of Federal Regulations
CFP	Communication Focal Point
CIO	Chief Information Officer
CITS	Combat Information Transport System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLIN	Customer Line Item Number
CMMI	Capability Maturity Model Integrated
CND	Computer Network Defense
CO	Contracting Officer
COI	Community of Interest
COMSEC	Communications Security
CONOPs	Concept of Operations
CONUS	Continental United States
COR	Contracting Office Representative
COTS	Commercial off-the-Shelf
CPARS	Contractor Performance Assessment Reporting System
CRYPTO	Cryptographic
CST	Client Support Technician
CTAPS	Contingency Theater Automated Planning System
CVS	Contractor Verification System
DAA	Designated Approval Authority
DARS	DoD Architecture Registry System
DBIDS	Defense Biometric Identification System
DBA	Database Administrator
DBT	Defense Business Transformation

DCID	Director of Central Intelligence Directive
DFARS	Defense Federal Acquisition Regulation Supplement
DHCP	Dynamic Host Configuration Protocol
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD information Systems Repository
DMM	Domestic Mail Manual
DMS	Defense Messaging System
DNI	Department of National Intelligence
DNS	Domain Name Service
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
DOL	Department of Labor
DRM	Data Reference Model
DSN	Defense Switched Network
DT	Development Team
DUNS	Data Universal Numbering System
DVSG	Digital Video Signal Generator
DW	Data Warehouse
EA	Enterprise Architecture
EASS	Enterprise Architecture and Services and Support
EC	Equipment Custodian
ECCB	Enterprise Configuration Control Board
ECO	Equipment Control Officer
EIA	Electronic Industries Association
EIT	Electronic and Information Technology
EL-CID	Equipment Location-Certification Information Database
E-mail	Electronic Mail
ESB	Enterprise Service Bus
ESD	Enterprise Service Desk
EST	Eastern Standard Time
ESTP	Enterprise Sequence Transition Plan
ESU	Enterprise Service Unit
ETL	Extract Translate and Load
ETM	Enterprise Telephony Management
EVT	Enterprise Vocabulary Team
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FDCC	Federal Desktop Core Configuration
FDO	Foreign Disclosure Office
FFP	Firm Fixed Price

FGC	Force Generation Center
FIPS	Federal Information Processing Standard
FM	Financial Management
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRB	Force Readiness Branch
FRRS	Frequency Resource Record System
FSO	Functional Security Officer
FTE	Full-time Equivalent ~~Employee~~
FTP	File Transfer Protocol
G&A	General and Administrative
GAL	Global Address List
GAO	General Accounting Office
GAO	Governments Accountability Office
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GDSS	Global Decision Support System
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GIG	Global Information Grid
GILS	Government Information Locator Service
GMF	Government Master File
GOTS	Government-off-the-shelf
GPO	Group Policy Object
GSA	General Service Administration
GWAC	Government Wide Acquisition Contracts
HCM	Human Capital Management
HCT	Human Capital Transformation
HP	Hewlett Packard
HQ	Headquarters
HQ USAF/RE	Headquarters United States Air Force, Office of Reserve Affairs
HQ AFRC	Headquarters Air Force Reserve Command
HQ AFRC/A1CC	Headquarters Air Force Reserve Director of Manpower, Personnel, and Services Classification and Position Management Branch
HQ AFRC/A6	Headquarters Air Force Reserve Command Director of Communications
HQ AFRC/A6OC	Headquarters Air Force Reserve Command Director of Communications Mission Systems Branch
HQ AFRC/SCOS	Headquarters Air Force Reserve Command Director of Communications Networks Division
HQ AFRC/A6XP	Headquarters Air Force Reserve Command Director of Communications Plans and Program Branch
HQ AFRC/A6XR	Headquarters Air Force Reserve Command Director of Communications Planning and Budget Execution Branch
HQ AFRC/IP	Headquarters Air Force Reserve Command Director of Information Protection Office
HQ AFRC/RMG	Headquarters Air Force Reserve Command Readiness Management Group

HQ ARPC	Headquarters Air Reserve Personnel Center
HTML	Hypertext Markup Language
IC	Intelligent Community
ICD	Intelligent Community Directive
IA	Information Assurance
IAO	Information Assurance Officer
IAW	In accordance with
ICM	Internal Control Measures
I-COOP	Interim Continuity of Operations Capability
IE	Internet Explorer (Microsoft)
IEEE	Institute of Electrical and Electronics Engineers
IM	Information Management
IMM	International Mail Manual
INOSC	Integrated Network Operations and Security Center
IOS	Internal Operating System
IPO	Information Protection Office
IPR	In-Progress Review
IPTV	Internet Protocol Television
IPV6	Internet Protocol Version 6
ISA	Internet Security and Acceleration (Microsoft)
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
IT	Information Technology
i-TRM	Info-structure Technology Reference Model
ITS	Information Transport System
ITSS	Information Technology Solutions Shop
ITU	International Telecommunications Union
IUID	Item Unique Identification
IWS	Installation Warning System
JCIAAM	Joint Common Information Assurance Assessment Methodology
JER	Joint Ethics Regulation
JET	Joint Environment Toolkit (weather system)
JIE	Joint Information Enterprise
JITC	Joint Interoperability Test Command
JP	Joint Publication
JPAS	Joint Personnel Adjudication System
JTR	Joint Travel Regulation
KEYMAT	Keying Material
LAN	Local Area Network
LMR	Land Mobile Radio
LRA	Local Registration Authority
MAJCOM	Major Command
MCCC	MAJCOM Communications Coordination Center
MCEB	Military Communications Electronic Board
MCSE	Microsoft ® Certified Systems Engineer
MFM	MAJCOM Functional Managers

MFS	Monthly Financial Summary
MIBS	Management Information Base
MIL-STD	Military Standards
NISPOM	National Industrial Security Program Operating Manual
MPF	Military Personnel Flight
MS	Microsoft
MSE	HQ MAJCOM Support Element
MS SCCM	Microsoft System Center Configuration Manager
MTO	Maintenance Tasking Order
MTS	Monthly Technical Summary
NAC	National Agency Check
NACLC	National Agency Check with Local Agency Check and Credit Check
NAS	Network Attached Storage
NAS	Naval Air Station
NCC	Network Control Center
NCDS	Net-Centric Data Strategy
NCSC	National Computer Security Center
NDI	Non-Developmental Initiatives
NESI	Net-centric Enterprise Solutions for Interoperability
NETOPS	Network Operations
NFS	Network File System
NIPRNET (NIPR)	Non-Secure Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLT	Not Later Than
NMS	Network Management System
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
NTIS	National Telecommunications and Information Systems
O&M	Operations & Maintenance
OCI	Organizational Conflict of Interest
OCS	Office Communications Server (Microsoft)
ODS	Operational Data Store
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
OPSEC	Operations Security
OSHA	Occupational Safety and Health Administration
OSI	Open Systems Interconnection
OV1	Operation's View 1
PAA	Privileged Access Agreement
PART	Program Assessment Rating Tool
PAoA	Preliminary Analysis of Alternatives
PC	Personal Computer
PEP	Project Execution Plan
PERL	Practical Extraction and Report Language
PEX	Patriot Excalibur

PGI	Procedures, Guidance, and Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMO	Program Management Office
POA&M	Plan of Action & Milestones
POC	Point of Contact
POE	Power over Ethernet
POP	Period of Performance
POV	Privately Owned Vehicle
PPIRS	Past Performance Information Retrieval System
PRI	Primary Rate Interface
PRM	Performance Reference Model
PWS	Performance Work Statement
QAP	Quality Assurance Personnel
QCP	Quality Control Plan
QOS	Quality of Service
R&D	Research and Development
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RMF	Risk Management Framework
RMS	Remedy Management System
ROI	Return on Investment
ROS	Report of Survey
SA	System Architecture
SANS	Storage Area Network
SAP	Special Access Program
SAR	Special Access Required
SATS	Supply Asset Tracking System
SCCM	System Center Configuration Manager (Microsoft)
SCIF	Sensitive Compartmented Information Systems
SOCE	Service Oriented Cloud Environment
SCOM	System Center Operations Manager
SCS	Spectrum Certification Software
SDA	System Design Alternative
SDC	Standard Desktop Configuration
SDDP	Service Development and Delivery Process
SFAF	Standard Frequency Action Format
SIP	Session Initiated Protocol
SIPRNET (SIPR)	Secure Internet Protocol Router Network
SMB	Server Message Block (protocol)
SME	Subject Matter Expert
SMO	Security Management Office
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOCE	Service Oriented Cloud Environment

SOP	Standard Operating Procedures
SPS	Standard Procurement System
SQL	Structured Query Language
SRM	Service Reference Model
SSL	Secure Socket Layer
STEM	System Telecommunications Engineering Manager
STIG	Security Technical Implementation Guide
STP	Spanning Tree Protocol
T&M	Time and Material
TASKORD	Tasking Orders
TASS	Trusted Associate Sponsorship System
TBA	Training Business Area
TCO	Technical Compliance Order
TCO	Telephone Control Officer
TCP/IP	Transmission Control Protocol/Internet Protocol
TCNO	Time Compliance Notification Order
TCNO	Time Compliance Network Order
TCTO	Time Compliance Technical Order
TDY	Temporary Duty
TF	Total Force
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TMAP	Telecommunications Monitoring and Assessment Program
TMG	Threat Management Gateway
TMT	Top Management Tool
TMS	Tasker Management System
TMS	Telecommunications Management System
TO	Technical Order
TPOC	Technical Point of Contact
TRM	Technical Reference Model
UCMJ	Uniformed Code of Military Justice
UDDI	Universal Description Integration
UMD	Unit Manning Document
UMPR	Unit Manpower Personnel Roster
US	United States
USAF	United States Air Force
UTA	Unit Training Assembly
UTAPS	Unit Training Assembly Participation System
VAL	Visitor Authorization Letter
VGSA	Visitor Group Security Agreement
VLAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
VoSIP	Voice Over Secure Internet Protocol
VPN	Virtual Private Network
VPS	Voice Protection System
VSS	Voice Switching System

VTC	Video Teleconferencing
WAN	Wide Area Network
WARNORDS	Warning Orders
WIN	Windows
WIPO	World Intellectual Property Organization
WWW	World Wide Web
XML	eXtensive Markup Language

TABLE 2
PUBLICATIONS USED IN DAILY OPERATIONS

Below is a list of publications and forms that are applicable to this PWS. NOTE: They are not all inclusive and are subject to change as they are revised and/or as guidance changes. The Contractor shall follow the applicable publications and forms to the extent and in the manner specified. All publications and forms are available on either the Air Force E-Publishing Website (www.e-publishing.af.mil) or the internet. However, in the event a publication and/or form is not available, the Government representative will work to provide a copy of the particular publication and/or form to the Contractor. (For more guidance, refer to para 5.18.)

- **Privacy Act of 1974**
- **Joint Publication (JP) 1-02,** ***Department of Defense Dictionary of Military and Associated Terms***
- **Joint Vision 2020 (current version)**
- **DODM 4525.6-M,** ***DoD Postal Manual***
- **DOD 4525.8-M,** ***DoD Official Mail Management***
- **DODD 4630.05,** ***Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)***
- **DoDI 4630.8,** ***Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)***
- **DoDI 5000.2,** ***Operation of the Defense Acquisition System***
- **DoDI 5120.4,** ***Department of Defense Newspapers, Magazines and Civilian Enterprise Publications***
- **DOD 5200.1-R,** ***DoD Information Security Program***
- **DoDM 5200.01V1,** ***DoD Information Security Program: Overview, Classification, and Declassification***
- **DoDM 5200.01V2,** ***DoD Information Security Program: Marking of Classified Information***
- **DoDM 5200.01V3,** ***DoD Information Security Program: Protection of Classified Information***
- **DoDM 5200.01V4,** ***DoD Information Security Program: Controlled Unclassified Information***
- **DoD 5200.2-R,** ***Personnel Security Program***
- **DoD 5200.08-R,** ***Physical Security Program***
- **DODI 5205.8,** ***Access to Classified Cryptographic Information***

- **DoD 5220.00-M,** ***Data Sanitization Method***
- **DoD 5220.22-M*, National Industrial Security Program Operating Manual & Sup 1***
- **DoD 5220.22-R, *Department of Defense Industrial Security Program***
- **DoDD 5200.28, *Security Requirements for Automated Information Systems (AIS)***
- **DoDD 5230.9, *Clearance of DoD Information for Public Release***
- **DoDD 5240.1, *Activities of DoD Intelligence Components that Affect United States Persons***
- **DoDI 5200.40, *DoD Information Assurance Certification and Accreditation Process (DIACAP)***
- **DoDD 5400.7, *DoD Freedom of Information Act Program***
- **DoD 5400.11-R, *Department of Defense Privacy Program***
- **DoDD 5400.11, *Department of Defense Privacy Program***
- **DoD 5500.7-R, *Joint Ethics Regulation (JER)***
- **DoD 7000.14-R, Volume 2A and 2B, *Department of Defense Financial Management Regulation***
- **DoDD 8000.1, *Management of the Department of Defense Information Enterprise***
- **DODD 8100.1, *Global Information Grid (GIG) Overarching Policy***
- **DODD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)***
- **DoDI 8100.3, *Department of Defense (DoD) Voice Networks***
- **DODD 8320.02, *Data Sharing in a Net-Centric Department of Defense***
- **DoDD 8320.2, *Information Sharing in a Net-Centric Department of Defense* (current version)**
- **DODI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property***
- **DoDD 8500.1, *Information Assurance***
- **DoDD 8500.2, *Information Assurance Implementation***
- **DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)***
- **DOD 8570.01M, *Information Assurance Workforce Improvement Program***
- **DoD 8910.1-M, *DoD Procedures for Management of Information Requirements***
- **DoDD 8910.1-M, *DoD Procedures for Management of Information Requirements***
- **DoD Radio Frequency Identification (RFID) Policy Memo, 30 Jul 2004**
- **CJCSM 3170.01C, *Operation of the Joint Capabilities Integration and Development System***
- **CJCSI 3170.01G, *Joint Capabilities Integration and Development System (JCIDS)***
- **CJCSI 6211.02C – *Defense Information System Network (DISN): Policy and Responsibilities***
- **CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities***
- **CJCSI 6215.01, *Policy for the Defense Switched Network***
- **CJCSI 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems***
- **CJCSI 6510.01, series, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)***

- **AFPD 10-7,** ***Information Operations***
- **AFI 10-701,** ***Operations Security (OPSEC)***
- **AFI 10-712,** ***Telecommunications Monitoring and Assessment Program (TMAP)***
- **AFMAN 14-304,** ***The Security, Use and Dissemination of Sensitive Compartmented Information (FOUO)***
- **AFPD 16-2,** ***Disclosure of Military Information to Foreign Governments and International Organizations***
- **AFMAN 23-110V2,** ***USAF Supply Manual***
- **AFI 23-111,** ***Management of Government Property in Possession of the Air Force***
- **AFMAN 23-220,** ***Reports of Survey for Air Force Property***
- **AFI 24-301,** ***Vehicle Operations***
- **AFPD 33-1,** ***Cyberspace Support***
- **AFI 31-101,** ***Integrated Defense***
- **AFI 31-113,** ***Installation Perimeter Control***
- **AFI 31-401,** ***Air Force Information Security Program***
- **AFI 31-501,** ***Personnel Security Program Management***
- **AFI 31-601,** ***Industrial Security Program Management***
- **AFI 33-106,** ***Managing High Frequency Radios, Personal Wireless Communication Systems, and the Military Affiliate Radio System***
- **AFI 33-112,** ***Information Technology Hardware Asset Management***
- **AFI 33-114,** ***Software Management***
- **AFI 33-115V1,** ***Network Operations (NETOPS)***
- **AFI 33-115V2,** ***Licensing Network Users and Certifying Network Professionals***
- **AFI 33-115V3,** ***Air Force Network Operating Instruction***
- **AFI 33-116,** ***Long-Haul Telecommunications Management***
- **AFI 33-119,** ***Air Force Messaging***
- **AFI 33-127,** ***Electronic Messaging Registration and Authority***
- **AFI 33-129,** ***Web Management and Internet Use***
- **AFI 33-150,** ***Management of Cyberspace Support Activities***
- **AFMAN 33-152,** ***User Responsibilities and Guidance for Information System*****s**
- **AFPD 33-2,** ***Information Assurance (IA) Program***
- **AFI 33-200,** ***Information Assurance Management***
- **AFI 33-201V1,** ***Communications Security (COMSEC)(FOUO)***
- **AFI 33-201V2,** ***Communications Security (COMSEC) User Requirements (FOUO)***
- **AFI 33-201V4,** ***Cryptographic Access Program (FOUO)***
- **AFI 33-201V5,** ***Controlled Cryptographic Items (CCI)(FOUO)***
- **AFI 33-201V7,** ***Management of Manual Cryptosystems (FOUO)***
- **AFI 33-201V9,** ***Operational Instructions for Secure Voice Devices (FOUO)***
- **AFI 33-210,** ***AF Certification and Accreditation (C&A) Program (AFCAP)***
- **AFI 33-230,** ***Information Assurance Assessment and Assistance Program***
- **AFI 33-214V1,** ***(S) Emission Security Assessment***
- **AFI 33-215,** ***Controlling Authorities for COMSEC Keying Material (KEYMAT)***
- **AFI 33-217,** ***Voice Call Sign Program***
- **AFMAN 33-282,** ***Computer Security (COMSEC)***

- **AFMAN 33-285,** ***Information Assurance (IA) Workforce Improvement Management***
- **AFPD 33-3,** ***Information Management***
- **AFI 33-322,** ***Records Management Program***
- **AFI 33-324,** ***The Air Force Information Collections and Reports Management Program***
- **AFMAN 33-326,** ***Preparing Official Communications***
- **AFI 33-332,** ***Air Force Privacy Program***
- **AFH 33-337,** ***The Tongue and Quill***
- **AFMAN 33-363,** ***Management of Records***
- **AFI 33-364,** ***Records Disposition-Procedures and Responsibilities***
- **AFI 33-580,** ***Spectrum Management***
- **AFI 35-109,** ***Visual Information***
- **AFI 38-501,** ***Air Force Survey Program***
- **AFI 40-102,** ***Tobacco Use in the Air Force***
- **AFPD 61-2,** ***Management of Scientific and Technical Information***
- **AFI 61-204,** ***Disseminating Scientific and Technical Information***
- **AFI 63-1201,** ***Life Cycle Systems Engineering***
- **AFI 65-503,** ***US Air Force Cost and Planning Factors***
- **AFI 71-101V2,** ***Protective Service Matters***
- **AFI 91-202,** ***The US Air Force Mishap Prevention Program***
- **AFI 91-203,** ***Air Force Consolidated Safety Instruction (*****paragraphs 6.2.1, 6.2.16 and 6.2.17)**
- **AFI 91-204,** ***Safety Investigation & Reports***
- **AFRIMS (Air Force Records Information Management System), website located at Robins**
- **Occupational Safety and Health Administration Standards (OSHA)**
- **TO 00-35D-54,** ***US Air Force Deficiency Reporting, Investigation, and Resolution (DRI&R) process***
- **TO 00-33A-1001,** ***Technical Manual, Methods and Procedures: General Communications Activities Management Procedures and Practice Requirements***
- **Allied Communications Publication (ACP) 123(A),** ***Common Messaging Strategy and Procedures***
- **ACP 133,** ***Common Directory Services and Procedures***
- **ACP 134,** ***Telephone Switchboard Operating Procedures***
- **AFKAG-1,** ***Communications Security (COMSEC) Operations***
- **AFKAG-2,** ***Air Force COMSEC Accounting Manual***
- **AFSSI 5004V1,** ***The Certification and Accreditation (C&A) Process***
- **AFSSI 5009,** ***Information Protection (IP) Interim Toolset***
- **AFSSI 5020,** ***Remanence Security (converts to AFMAN 33-224)***
- **AFSSI 5021,** ***Vulnerability and Incident Reporting (converts to AFMAN 33-225v2)***
- **AFSSM 5022,** ***Network Risafssik Analysis Guide***
- **AFSSI 5023,** ***Virus and Other Forms of Malicious Logic***
- **AFSSI 5024V3,** ***The Designated Approving Authorities Handbook***
- **AFSSI 7010, (S) Emission Security Assessment (will convert to AFMAN 33-214V1)**
- **AFSSI 7700,** ***Emission Security (EMSEC)***

- **Air Force FAR Supplement (AFFARS)**
- **CIAC-2305 R.1, *UNIX Incident Guide: How to Detect an Intrusion***
- **CSC-STD-002-85, *Department of Defense Password Management Guideline***
- **Director of Central Intelligence Directive (DCID) 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)***
- **Executive Order 12958, *Classified National Security Information***
- **Federal Information Processing Standards (FIPS)**
- **FIPS) Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification***
- **FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control***
- **FIPS Pub 140-2, *Security Requirements for Cryptographic Modules***
- **FIPS Pub 192, *Application Profile for the Government Information Locator Service (GILS)***
- **Public Law 96-511, *The Paperwork Reduction Act of 1980, as amended 1986, Title 44, United States Code, Chap 35***
- **Public Law 100-235, *Computer Security Act of 1987***
- **National Telecommunications and Information Systems (NTIS) Security Directive No. 600, *Communications Security (COMSEC) Monitoring***
- **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Guide to *Information Technology Security Services***
- **NCSC-TG-017, *A Guide to Understanding Identification & Authentication in Trusted Systems***
- **Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources***
- **STIGS (DoD Security Technical Implementation Guides) and Checklists**
- **USCyber Orders**
- **Information Assurance Vulnerability Notices**
- **AF IT Lean Reengineering and SISSU Guidebook v5.0, (current version)**
- **American National Standards Institute (ANSI) Documents**
- **ANSI/TIA/EIA-568-A, Commercial Building Telecommunications Cabling Standard**
- **ANSI/TIA/EIA-568-A-1 Propagation Delay and Delay Skew Specifications for 100 4-pair Cable**
- **ANSI/TIA/EIA-569-1990, Commercial Building Standard for Telecommunications Pathways and Spaces**
- **TIA/EIA Standard-SP-3490 DRAFT 11, Residential Telecommunications Cabling Standard**
- **ANSI/TIA/EIA-606-1993, Administration Standard for the Telecommunications Infrastructure of Commercial Building**
- **ANSI/TIA/EIA-607-1994, Commercial Building Grounding and Bonding Requirements for Telecommunications**
- **CAM 09-39**
- **Combat Information Transport System (CITS) – Information Transport System (ITS) Architecture**
- **Computer Fraud and Abuse Act of 1986**

- **CND Directives as directed by USCYBERCOM**
- **Code of Federal Regulations (CFRs)**
- **Data Interchange Standards Community (E-Business)**
- **Defense Federal Acquisition Regulation Supplement (DFARS)**
- **Defense Information Systems Agency ATM and Voice Specification Standards**
- **DFARs and Procedures, Guidance, and Information (PGI)**
- **DISA Circular 310-M70-87,** ***Methods and Procedures Operational Policies and Procedures for the Defense Messaging System (DMS)***
- **DISA Concept of Operations (CONOPS)**
- **DISA and CSIP (Cyber Security Inspection Program)**
- **DISA STIG,** ***Application Security and Development***
- **DOD CIO Memorandum,** ***Department of Defense Information System Standard Consent Banner and User Agreement, 9 May 08***
- **DoD CIO Department of Defense Net-Centric Data Strategy, 9 May 2003**
- **DoD Discovery Metadata Specification (DDMS Version; (current version)**
- **DoD Enterprise Architecture (EA) Data Reference Model (DRM) DoD Enterprise Architecture Technical Reference Model**
- **DoD IPv6 Memorandum, June 9, 2003, and DoD CIO IPv6 Memorandum, 29 September 2003**
- **DoD IPv6 Generic Test Plan, Version 3**
- **DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 2 DoD IT Standards Registry (DISR)**
- **DoD Open Technology Development Guidebook**
- **Electronic Industries Association (EIA) Standards**
- **Electronic Industries Association (Alliance)**
- **Federal Acquisition Regulation (FAR)**
- **Federal Telecommunications Recommendation 1090-1997, Commercial Building Telecommunications Cabling**
- **Global Information Grid (GIG)**
- **Info-structure Technology Reference Model (i-TRM)**
- **Industry Best Practices in Achieving Service Oriented Architecture (SOA), 22 April 2005**
- **Institute of Electrical and Electronics Engineers (IEEE) Standards**
- **International Standards Organization (ISO) Documents**
- **International Committee for Information Technology Standards**
- **International Telecommunications Union ITU**
- **Joint Common Information Assurance Assessment Methodology (JCIAAM)**
- **Joint DoD/Department of National Intelligence (DNI) Federated Search Specification**
- **Joint Interoperability Test Command (JITC) Requirements**
- **JTF-GNOP WARNORD 07-37, Public Key Infrastructure Implementation Phase 2 (current version)**
- **Military Standards, Specifications, and Regulations (MIL-STDs, DoD-STDs)**
- **National Computer Security Center (NCSC) Documents**

- **National Institute for Standards and Technology (NIST) (formerly National Bureau of Standards, NBS) Documents**
- **National Security Agency Guidelines**
- **National Security Agency Rainbow Series**
- **Net-centric Enterprise Solutions for Interoperability (NESI)**
- **Net-Centric Operations & Warfare Reference Model**
- **Net-Centric Data Strategy (NCDS)**
- **NIST Special Publication 800-5, *Guide to the Selection of Anti-Virus Tools and Techniques***
- **OASD Net-Centric Checklist, Ver. 2.1.3, 12 May 2004**
- **OMB 95-01, *Establishment of the Government Information Locator Service***
- **Security Technical Implementation Guides (STIGS)**
- **SMI-ELS Strategic Concept V1, 1 September 2009**
- **Tasking Orders (TASKORDS)**
- **The Common Criteria Evaluation and Validation Scheme TIA/EIA-TSB-67, Transmission Performance Specifications for Field testing of Unshielded Twisted-Pair Cabling Systems**
- **TIA/EIA-TSB-72, Centralized Optical Fiber Cabling Guidelines**
- **TIA/EIA-TSB-75, Additional Horizontal Cabling Practices for Open Offices**
- **Title 5, Code of Federal Regulations, Part 1320, *Controlling Paperwork Burdens on the Public***
- **TL9000 Quality Management System QuEST Forum**
- **Uniform Code of Military Justice (UCMJ), Article 92**
- **USAF Black Voice Switching Systems Strategy**
- **USAF Black Voice Switching System Profile**
- **Warning Orders (WARNORDS)**

FORMS USED IN DAILY OPERATIONS

DEPARTMENT OF DEFENSE FORMS

DD 254	**DoD Contract Security Classification Specifications**
DD 1172-2	**Application for Identification Card/DEERs Enrollment**

AIR FORCE FORMS

AF 9	**Request for Purchase**
AF 649	**Verification of Long Distance Telephone Calls**
AF 833	**Multimedia Work Order**
AF 1297	**Temporary Issue Receipt**
AF 2005	**Issue/Turn-In Request**
AF 2583	**Request for Personnel Security Action**
AF 2586	**Unescorted Entry Authorization Certificate**
AF 2587	**Security Termination Statement**
AFCOMSEC 9	**Cryptographic Access Certificate (PA) (FOUO)**
AFCOMSEC 16	**COMSEC Account Daily Shift Inventory**
AFTO 95	**Significant Historical Data**

STANDARD FORMS

SF 85P	**Questionnaire for Public Trust Positions**
FD 258	**Fingerprint Card**
SF 312	**Classified Information Nondisclosure Agreement**
SF 701	**Activity Security Checklists**

~~TABLE 3~~
~~TYPES OF SERVICE~~

~~IT Support~~	~~GCCS~~	~~Staff Support~~
~~At multiple locations (See Table 4)~~	~~At HQ AFRC~~	~~At HQ AFRC (See Table 5)~~
~~Approx 116 FTE's (46 Robins, 70 other bases)~~	~~4 FTE's at Robins~~	~~16 FTE"s at Robins~~

~~TABLE 4~~
~~LOCATIONS AND TYPE OF IT SUPPORT~~

~~Location~~	~~LAN Admin~~	~~CFP~~	~~Public Key~~	~~Net Config~~	~~Infrastructure~~	~~Wireless~~	~~VTC~~	~~Switch Tech/ VOIP Network~~	~~FTE's ESTIMATED~~
~~AFRC – Robins AFB, GA~~	(b) (4)								(b) (
~~ARPC – Buckley AFB, CO~~	(b) (4)								(b) (
~~Pentagon – Washington D.C.~~	(b) (4)								(b) (
~~301 AW – NAS JRB Ft Worth (Carswell JRB), TX~~	(b) (4)								(b) (
~~304 RS – Portland IAP, OR~~	(b) (4)								(b) (
~~434 AW – Grissom ARB, IN~~	(b) (4)								(b) (
~~439 AW – Westover ARB, MA~~	(b) (4)								(b) (
~~440 AW – Pope Field, NC~~	(b) (4)								(b) (
~~919 CS – Duke Field, FL~~	(b) (4)								(b) (
~~452 AW – March ARB, CA~~	(b) (4)								(b) (
~~482 AW – Homestead ARB, FL~~	(b) (4)								(b) (
~~910 AW – Youngstown ARB, OH~~	(b) (4)								(b) (
~~911 AW – Pittsburgh ARS, PA~~	(b) (4)								(b) (
~~TOTAL FTEs~~	(b) (4)								(b) (4)

~~Total Table 4~~

(b) (4) ~~; not Including the~~ (b) (4) ~~for Robins listed in Table 3.~~

~~NOTE: March AFB~~ (b) (4) ~~EA, Storage Technician also. Total of~~ (b) (4 ~~FTE's at March.~~
~~GCCS in Table 3, not shown in Table 4.~~

~~TABLE 5~~
~~HQ STAFF SUPPORT~~

	~~SME (Subject Matter Expert)~~	~~Analyst~~	~~Action Officer~~	~~Functional Admin/Manager~~	~~ESTIMATED FTE~~
~~A6O~~	~~X~~		~~X~~		~~2~~
~~A6X~~	~~X(2)~~	~~X(8)~~		~~X(2)~~	~~12~~
~~SC~~			~~X(2)~~		~~2~~
~~Total FTEs~~	~~3~~	~~8~~	~~3~~	~~2~~	~~16~~

~~Total: 16 (see table 3)~~

~~GCCS in Table 3 indicates 4 FTE's. This corresponds to PWS Para's 3.3, 3.4 and 3.5 . PWS breakout is for government funding purposes.~~

~~TABLE 6~~
~~VTC ESTIMATED MONTHLY WORKLOAD~~

~~Engineering / Maintenance~~	~~120 hours~~
~~Video Teleconferences~~	~~186 hours~~
~~Support & Facility endpoints~~	~~52 hours~~
~~Local Presentations~~	~~750 hours~~
~~Scheduling VTC~~	~~90 hours~~

~~TABLE 7~~
~~POPULATION SUPPORT~~

~~LOCATION~~		~~POPULATION~~
~~AFRC Robins~~		~~2,247~~
~~HQ ARPC – Buckley AFB, CO~~		~~550~~
~~94 AW – Dobbins ARB, GA (In-sourced, MSE and ASE support only; no on-base support)~~		~~2,201~~
~~301 AW – NAS JRB Ft Worth (Carswell JRB), TX~~		~~2,097~~
~~304 RS – Portland IAP, OR~~		~~94~~
~~434 AW – Grissom ARB, IN~~		~~1,768~~
~~439 AW – Westover ARB, MA~~		~~2,687~~
~~440 AW – Pope Field, NC~~		~~4,500~~
~~452 AW – March ARB, CA~~		~~4,001~~
~~482 AW – Homestead ARB, FL~~		~~1,857~~
~~910 AW – Youngstown ARB, OH~~		~~1,678~~
~~911 AW – Pittsburgh ARS, PA~~		~~1,562~~
~~914 AW – Niagara Falls AFS, NY (In-sourced, MSE and ASE support only; no on-base support)~~		~~1,522~~
~~919 SOW – Duke Field, FL~~		~~UNK~~
~~934 AW – Minn St Paul, MN (In-sourced, MSE and ASE support only; no on-base support)~~		~~1,594~~
~~Total Population Supported~~		~~23,858~~ ~~28,358~~

TABLE 8
REQUEST FOR CAC

MEMORANDUM FOR 951 RSPTS/CSS

FROM: Quality Assurance Personnel (QAP) – Service Requirement Originating Office
HQ AFRC/SCXP
David Williams

SUBJECT: Trusted Agent Authorization to Issue Common Access Card (CAC)

1. The individual listed below is a contractor employee directly supporting my organization under the contract indicated. The individual will require a CAC card, as his/her duties require access to **Robins Air Force Base**.

Signature & Date of Government: ________________________________

Name (last, first): ______________________ **SSN:** _______________

Date of Birth (mm/dd/yyyy): ________________

Contact Email Address: _____________________________

Company Name: __________________________________

Contract Number and Expiration Date: 4QBA57113850 / __________________

Organization and Program Support: _______________________________________

Work Location: _____________________________

Security Investigation Status: _____________________________
(NOTE: DoD requirements state that all persons issued a CAC will have a minimum of a Security Background Investigation submitted. A favorable completed security clearance investigation satisfies this need. Consult your security manager for specific requirements)

2. I certify the contract identified in part I above was awarded in support of the service requirement organization office on ______________ and the individual named will require a CAC card as his duties require access (insert the base/installation). If any additional contract information is needed, please contact me at _______.

David Williams, GS-13, USAF
Contracting Officer Representative (COR) Alternate